UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

JOSHUA ADAM SCHULTE,
Plaintiff

-v-

UNITED STATES OF AMERICA,
Defendant.

22-CV-05841
(EK) (RML)

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF JOSHUA ADAM SCHULTE'S MOTION FOR RETURN OF STOLEN PROPERTY PURSUANT TO FED. R. CRIM. P. 41(g)

Joshua Adam Schulte, pro se
MDC
P.O. Box 329002
Brooklyn, NY 11232

TABLE OF CONTENTS

I. PRELIMINARY STATEMENT

The FBI executed a warrantless search of Mr. Schulte's Discovery laptop on June 3, 2022, and then lied in a search warrant affidavit about the interpretation of what it found in that warrantless search to seize the laptop on July 27, 2022. Despite no legitimate reason to do so, the government then executed a general warrant, and went well beyond the false probable cause described in the illegal warrant, and began an exhaustive search of all the files on the laptop for anything that may resemble a crime—and specifically, to review pictures and videos despite no legitimate reason to do so. After approximately two months of this ever-broadening exhaustive search, the government claimed to find child pornography on the laptop and filed for another three[1] search warrants. However, the government once again lied in its affidavits, as the alleged child pornography was actually adult pornography produced by the government to Mr. Schulte pursuant to Fed. R. Crim. P. 16 in United States v. Schulte, 17 CR 548(JMF). Finally, in the second Eastern District warrant issued on October 4, 2022, the government searched beyond the terms of the particularly described place, and unlawfully seized three hard drives; the government also searched and seized papers and notebooks despite failing to establish that Mr. Schulte possessed papers and notebooks, much less that there was any probable cause to search them. Accordingly, both the July 26, 2022 search warrant executed on July 27th and the October 4, 2022 search warrant executed on October 5th violate the Fourth Amendment, and all illegally stolen items must be returned in accordance with Fed. R. Crim. P. 41(g).

1 There are a total of four unconstitutional search warrants, but only two issued in the E.D.N.Y. This motion only seeks return of the items seized in the E.D.N.Y. warrants pursuant to Fed. R. Crim. P. 41(g) ("The motion must be filed in the district where the property was seized").

II. STATEMENT OF FACTS

A week before trial was to begin in U.S. v. Schulte, the BOP dropped and damaged Mr. Schulte's laptop, who was representing himself. See Dkt. 838. At a June 3, 2022 hearing, the government proposed to "assist" in swapping the hard disk drive to that of the new laptop purchased by Standby Counsel. Mr. Schulte wearily agreed under very strict conditions that the government ① only perform a swap of the laptop's hard drive, ② not conduct any search, and ③ not alert the prosecutors to any incidental disclosures. There was a colloquy on the record to this effect issued by U.S.D.J. Jesse M. Furman. See exhibit A. Upon receipt of the laptop, the government immediately violated all three conditions by ① attempting to power on the laptop, ② searching the BIOS, ③ logging into the laptop, ④ searching the laptop, and ⑤ notifying the prosecutors of their findings: an unprivileged BIOS password and a small encrypted drive on the laptop. The government complained to the judge at the same hearing, lying and claiming that the laptop was potentially compromised by the unprivileged BIOS password. However, the government did not obtain a warrant, but ultimately returned the laptop to Mr. Schulte AFTER verifying the BIOS integrity.

During the trial, Mr. Schulte provided the government with defense exhibits 1210 and 1211, which were source code and a compiled program that could modify the file times on a Windows computer. The exhibits were critical to the defense to demonstrate that the filetimes of the backups of CIA source code allegedly stolen by Mr. Schulte could have easily been modified. This line of questioning was used at the first trial in 2020 by attorney Sabrina Shroff, and Mr. Schulte hoped to improve upon it at the retrial. The government complained to the judge, lying and claiming that this meant Mr. Schulte could write malware and compromise the discovery laptop. However, the government did not obtain a search warrant, and the trial continued. The disputed exhibits were shown to the governments experts, and the line of questioning posed, but the exhibits were not ultimately introduced at trial.

A few weeks after trial, on July 26, 2022, the government deliberately and maliciously lied in a search warrant affidavit to seize the laptop, and executed the illegal search the next day. See Ex. B.

The government's illegal search warrant purported to establish probable cause that the BIOS was modified to allow the laptop to connect to the internet. Even if this were considered a lawful search, based upon the scant probable cause the government was only authorized to search the BIOS to determine whether the wifi adapter had ever been enabled—and at the very most, examine Microsoft Windows files to determine if and when the laptop had ever been connected to the internet. Instead, the government executed a general warrant and searched every single byte of the laptop—reviewing Mr. Schulte's files, including pictures and videos.

Based upon this overbroad search, the government pretended it found hundreds of child pornography pictures and videos. It then filed three additional search warrants to ① conduct a child pornography search on the laptop (9/23/22), ② seize Mr. Schulte's Discovery Drives (10/4/22), Ex. C, and ③ seize Mr. Schulte's devices at the courthouse SCIF.

All four search warrants are void because ① they relied upon evidence obtained from a warrantless search, ② are predicated on reckless misstatements, deliberate lies, and omissions of material facts, ③ were overbroad with respect to the established facts from which the search warrants were based, inter alia. Accordingly this court should find the two Eastern District searches, to which it has jurisdiction, unconstitutional; all unlawfully seized materials must be returned to Mr. Schulte.

III. FED. R. CRIM. P. 41(g)

The Fourth Amendment guarantees that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. "[N]o warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Id.

For a warrant to issue, a magistrate must make a 'practical, common-sense decision whether, given all the circumstances set forth in the affidavit... there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" Illinois v. Gates, 462 U.S. 213, 238 (1983); see also United States v. Raymonda, 780 F.3d 105, 113 (2d Cir. 2015).

"Rule 41(g) permits a person aggrieved by the government's unlawful seizure or deprivation of property to move for specific relief: the property's return." Adeleke v. United States, 355 F.3d 144, 149 (2d Cir. 2004). "[W]here no criminal proceedings against the movant are pending or have transpired, a motion for the return of property is treated as a civil equitable proceeding." Mora v. United States, 955 F.2d 156, 158 (2d Cir. 1992) (internal quotation marks, citation, and alterations omitted).

To prevail on a Rule 41(g) motion, the claimant must demonstrate that (1) he is entitled to lawful possession of the seized property; (2) the property itself is not contraband; and (3) either the search was illegal or the government's need for the property as evidence has ended. Ferreira v. United States, 354 F.Supp. 2d 406, 409 (S.D.N.Y. 2005).

There can be no question that the discovery laptop purchased by Mr. Schulte and provided by the government, as well as the discovery drives purchased and provided by the government and Mr. Schulte's notebooks and paper documents are not contraband, and Mr. Schulte is entitled to lawful possession of these items—particularly his work product and data stored on the electronic devices. Accordingly, the remainder of this motion focuses on the clear fact that the government's searches were unconstitutional.

P.5 A. The July 26, 2022 MDC Seizure of the laptop was Unconstitutional

1. The June 3, 2022 warrantless search

Right before trial the BOP dropped Mr. Schulte's laptop, rendering it inoperable. Standby counsel immediately purchased a new laptop, and at the June 3, 2022 CIPA hearing the government agreed to remove the old drive. See Ex. A, 6/3/22 Tr. Mr. Denton notified the Court that "the U.S. Attorney's office is going to take possession of the defendant's broken laptop in the interests of trying to have our IT staff execute this hard drive swap with the replacement as soon as possible it's available." Tr. 110. Mr. Denton further states "We just wanted to make sure there was some record the defendant was aware of it and consented to us doing that." Id. the COURT states: "Ok. I'm guessing his consent may be contingent on this. I assume it goes without saying that the contents would not be viewed by anyone, but certainly not by anyone associated with the trial team in any way, shape, or form?" Id. Mr. Denton then answers: "Only the IT staff as necessary to assure accomplishment of the objective." Id. 110-111. Then:

THE COURT: Ok. Mr. Schulte?

THE DEFENDANT: IT staff should not talk to him, but yes.

THE COURT: I think that was implicit in what Mr. Denton was saying. Just to make it explicit, I take it, Mr. Denton, you would represent that no one on the trial team will know anything one way or another about the contents of the laptop, other than the mere fact that it did or didn't work to transfer?

MR. DENTON: Certainly not, your Honor

THE COURT: Mr. Schulte, with that understanding?

DEFENDANT: Yes.

MR. LOCKARD: One additional clarification. They said they may need the log-in information in order to make the transfer happen or swap the hard drives. So, Mr. Denton and I don't need the log-in information. Our IT staff would like the log-in information so they can do this.

THE DEFENDANT: I'll authorize standby counsel, if needed. I don't think it shouldn't be needed for swapping the stuff. If so, standby counsel can speak with them and give it to them.

Accordingly, the authorization granted by Mr. Schulte was very clearly defined: the government can remove the physical hard drive for transfer into the new laptop. That's it. The government was not authorized to even attempt to power on the laptop, and certainly not to conduct searches of the BIOS or drive contents; furthermore, in case IT staff incidentally stumbled upon anything, they were not authorized to inform the government — As Judge Furman reiterated, "no one on the trial team will know anything one way or another about the contents of the laptop."

A search must not exceed the scope of the consent given. Florida v. Royer, 460 U.S. 491, 500-01 (1983). To determine the parameters of consent, courts "ask 'what would the typical reasonable person have understood by the exchange between the officer and the [consenting party]?'" Winfield v. Trottier, 710 F.3d 49, 55 (2d Cir. 2013) (quoting Florida v. Jimeno, 500 U.S. 248, 249 (1991)). "The scope of a search is generally defined by its expressed object." Id. (quoting Jimeno, 500 U.S. at 251); United States v. Ross, 456 U.S. 798 (1982). The ultimate question is "whether the officer had a reasonable basis for believing that there had been consent to the search." U.S. v. Sanchez, 32 F.3d 1330, 1334-35 (8th Cir. 1994) (collecting cases).

What would the typical reasonable person have understood by this on-the record exchange? Mr. Schulte did not request the government to troubleshoot or fix the laptop; he merely requested that they physically remove the hard drive to place it, physically, into the new laptop. This is a "hard drive swap" as stated on the record by Mr. Denton. This does not require the government to power on the laptop — hence Mr. Schulte's statement on-the-record that any password should not be necessary. And what does the statement "IT staff should not talk to him [Denton]" or "no one on the trial team will know anything one way or another about the contents of the laptop"? Do these statements mean that the government should search the laptop and report its findings to the prosecutors? Of course not — No search. No report. The scope of consent is critically important, because without it — there would be no search. If Mr. Schulte knew the government would search the laptop then he never would have agreed for their possession; this arrangement only existed because it was the eve of trial and Mr. Schulte's experts were out-of-pocket. Otherwise, the defense team would have performed the hard drive

swap. Instead, due to the exigencies, the government "offered" its "assistance" in lieu of postponing trial. And Mr. Schulte agreed to this "assistance" provided they merely perform this one task — a simple hard drive swap — not power on or search the laptop.

Mere seconds after receiving the laptop, the government immediately violated ALL the terms of the laptop transaction; they powered up the laptop and began searching notwithstanding the aforementioned scope. See, e.g.: 6/3/22 Tr. at 174-75:

MR. LOCKARD: "So the update is that our IT staff was able to power up the computer. It did boot up. They are unable to log in to check to see if the hard drive is working. The password they received did not work.

"So the request from Mr. Schulte is, can we get the correct password for the laptop. The second part of the update is that when the IT personnel did boot the computer up, it appeared to them that the bios configuration had been changed. The bios configuration, my understanding that that is the system that runs the hardware and the ports and things like that, in way that they can no longer confirm if the laptop is compliant with BOP and DOJ security requirements."

Mr. Schulte never consented for the government to power on or troubleshoot the laptop. Mr. Schulte and the Court explicitly stated that the government was to perform a hard drive swap — and that the IT were forbidden from performing a search or notifying the government of any incidental findings; yet the government disregarded all this and simply did as it pleased.

From there, it further spiraled into a demand for, and ultimately coerced password Seizure and an even more extensive, warrantless search of the laptop. The government's request for the password to "check to see if the hard drive is working" was obviously ludicrous — if the laptop boots then obviously the hard drive is working since the operating system is installed on the hard drive and cannot boot if the hard drive is dysfunctional as even a senile old man knows. So, this was a veil to obtain the password for nefarious purposes instead. Mr. Schulte did NOT consent, and instead requested "is there any way, after this is over, that they can bring the laptop, and standby counsel and myself can look through it to see if it's been reset, or if is that acceptable?" The government refused and demanded the password because as Mr. Brent Lockard stated, "I think in light of the concern about the configuration settings, our IT needs to make sure that it is

P. 8 still configured appropriately for being able to be in BOP space and used by an inmate." Id. at 176. So, after violating the scope of consent, the government then demanded the password before they would return the laptop — but this of course made no sense since the BIOS settings are independent from the operating system, as will be discussed in the next section. In the end, the government obtained the password and conducted a warrantless search of the laptop — ultimately "discovering" the encrypted drive and then notifying the prosecutors.

As for the miraculous recovery of the laptop, the government asserted that indeed the laptop was not broken at all, but simply used the "wrong" power cable. This power cable was provided by the manufacturer, used the correct output voltage/current, and worked perfectly fine for ~~one~~ over a year. Moreover, this explanation is not adequate to explain how the laptop at full charge no longer functioned after dropped by MDC — who confirmed that they dropped the laptop and that their staff were unable to "repair" the laptop. See, e.g. Dkt. 838.

Regardless of these suspicious circumstances surrounding the laptop's demise and miraculous recovery by government IT staff who simply powered it on "with a different power cable", the fact remains that the government was specifically not authorized to power on the laptop — only to physically remove the hard drive. Id. as referenced, the law is quite clear when the government goes beyond the scope authorized — this is no different from a warrantless search, which is prohibited by the Fourth Amendment. This unlawful, warrantless search nullifies any and all findings from the search; they are considered fruits of the poisonous tree. Since the initial search warrant to seize the laptop on June 27, 2022 contained nothing but fruit of the poisonous tree, the Court need not turn another page as that immediately ends the analysis and renders all searches in violation of the Fourth Amendment and unconstitutional; the devices must be returned immediately.

Finally, it should be noted that even if the government argues it was trying to be helpful by troubleshooting the laptop, this is no excuse for violating the scope; furthermore, upon discovering a working laptop, the government should have immediately ended its already-illegal-search to notify and return the laptop. The fact that they not only failed to do so, but instead proceeded to log into and search the laptop demonstrates bad faith and treachery by the government.

P.9

2. The "modified" BIOS: the government's reckless disregard of the truth

a. BIOS – what is it?

See Ancora Techs, Inc. v. Apple, Inc., 2012 U.S. Dist. LEXIS 183045 (N.D. Cal, Dec. 31, 2012) at 17-18: "The Microsoft Computer Dictionary, 5th Edition, 2002, BIOS, n. Acronym for basic input/output system. On PC-compatible computers, the set of essential software routines that tests hardware at startup, starts the operating system, and supports the transfer of data among hardware devices, including the date and time... The BIOS is stored in read-only memory (ROM) so that it can be executed when the computer is turned on. Although critical to performance, the BIOS is usually invisible to computer users."

Essentially, the BIOS is an operating system stored in an immutable persistent chip on the computer itself (not on any hard drive) that first executes when the computer is turned on. Its primary function is to check the hardware, allow the user to configure certain devices, detect a particular hard drive boot sector, load the operating system into memory, and pass the configured devices and control to that operating system — in this case Microsoft Windows.

The BIOS allows you to enable or disable devices. Particularly relevant here is the wifi adapter. Every modern laptop has a built-in wifi card. Since the BOP does not allow the use or access of the internet, the government disables the wifi card in the BIOS; so on boot, the BIOS does not pass the wifi adapter to Windows, and therefore Windows "believes" there is no wifi card at all — Windows only "knows" the devices on any computer based on what the BIOS tells it. Another configuration option the government used is known as "Secure Boot" which basically locks the device that the BIOS passes control to on boot, thereby preventing boot from an external hard drive or thumbdrive.

Finally, it should be noted that the BIOS is obviously independent from any particular hard drive or operating system and maintains its own access controls — meaning the BIOS cannot be accessed or modified from a Windows account or session. Not even a Windows administrator account can access or modify the BIOS — only a BIOS account accessed by pressing a specific key when the computer is first turned on but before boot of the OS ("hit del to enter setup"). Every modern laptop provides at least two BIOS accounts — a privileged account that can modify the BIOS configuration and an unprivileged view account that allows everyone to review the current BIOS configuration, but not modify it.

P.10

b. The government's allegations concerning the BIOS

The government outlines its allegations concerning the BIOS on pages 13-14 (JAS 028181-82) of the 7/27/22 search warrant (Ex. B). The government claims that it "physically disconnected the wires connecting the wifi adapter from the motherboard" (i.v), that the laptop bootup BIOS login screen was for a user account which was not created by IT staff when the laptop was setup, but that IT staff were "able to log in to the BIOS and access the Windows operating system using an administrator password, but did not have access to the changed user password." (i.vi), and finally "IT staff did not review whether BIOS settings for the [laptop] had been changed or whether the wireless capability had been reconnected to the motherboard (i.v). The majority of these claims are outright fabrications, falsifications, and a fraud on the Court.

c. The government perpetrated a fraud on the court by claiming it never checked the BIOS settings when in reality it refused to return the laptop until IT checked and verified the BIOS integrity. There can be no mistake that the government's claim in t.iv (p. 13-14) that "IT staff did not review whether BIOS settings for the [laptop] had been changed or whether the wireless capability had been reconnected" is a total fraud upon this Court. The transcripts from June 3rd plainly show the complete opposite — that the government refused to return the laptop until its IT department confirmed that the BIOS settings were unaltered and that the laptop complied with BOP guidelines — i.e. no internet access. Specifically, I refer the Court to page 175 of the 6/3 transcript and the quoted statement of Mr. Lockard as recanted herein on page 7 of this motion; but particularly to his final statement: "So if we do get the correct passwords, they will be able to confirm or reset the security settings so that the laptop can go back to the MDC with Mr. Schulte." Furthermore, Judge Furman asked "[T]he suggestion being that Mr. Schulte altered the bios settings, whatever that may be?" To which Mr. Lockard replied "[y]our Honor, we are making no inferences. He's had the laptop a long time. They would like to reconfirm the configuration." The Court then goes on to request this procedure specifically. See, e.g. 6/3/22 Tr. at 177-78:

THE COURT: "... I certainly agree, if the BIOS configuration is not what BOP and protective order requires, then that should be conformed to what it does require, without intimating who did what. Bottom line is, first step is to get access to the computer. Hopefully we can resolve it here now."

P.11 MR. LOCKARD: "Yes. Our goal is to make sure it's compliant, get it fixed, back to Mr. Schulte. If he writes down the password, I'll hand it back to the paralegal to take to the IT department."

The CIPA hearing proceeded until the end—during which time the government's IT staff confirmed that the BIOS settings were unmolested and that the wifi adapter was not functional; the password for the unprivileged BIOS account was confirmed as configured by the IT department and left alone. The fully compliant laptop was then returned to Mr. Schulte. Thus the government's 7/22/22 search warrant affidavit is exposed as the outrageous fabrication that it is; the government clearly perpetrated a fraud on this court, lying to the face of magistrate Pollak.

d. The government lied by not explaining the impact of disconnecting the wifi card

The government state in their fraudulent affidavit that the "IT staff physically disconnected the ~~[illegible]~~ wire connecting the wifi from the motherboard of the [laptop]" but dont elaborate and explain this significance. The BIOS controls devices connected to the motherboard—if a device is not physically connected, then the BIOS—and the ability to modify its configuration—is completely irrelevant. Even if an attacker were able to "hack" the BIOS, they still could not enable the wifi capability since it was not physically connected.

Moreover, the wifi card is not connected with mere cables, but is physically soldered onto the motherboard. Furthermore, to get into the hardware of the laptop requires bypassing at least 6 screws of the special diamond security rivet—requiring a specialized screwdriver. Mr. Schulte is held in a maximum security SAMs unit with 24/7 monitoring—he is forbidden from accessing his own light let alone a screwdriver or even specialized screwdriver. Hence, to reconnect the wifi, Mr. Schulte (1) would need to know that the adapter was physically disconnected, (2) ~~[illegible]~~ acquire a specialized screwdriver, (3) open up the laptop, (4) identify the wifi card, (5) identify where on the motherboard it had been sabotaged, (6) acquire a soldering iron, (7) connect the soldering iron to a power outlet (no cells in his unit or any maximum security SAMs unit have power outlets), and (8) solder the wifi back to reconnect it; he must do all this while recorded 24/7 by camera and inspected every 15 minutes by the unit officer. Due to the complexity required not only in resources but skill, this is a practical impossibility. Since this action must be taken to reenable the wifi capability and since the government possesses all video of Mr. Schulte in his cell, it was required to review and show the court this impossible event before probable cause could be established.

c. The government lied by not explaining BIOS access controls

The affiant deliberately misled the Court with reckless disregard for the truth by failing to explain the different BIOS access controls. The BIOS is configured with two accounts— a privileged administrator account and an unprivileged account. Only the privileged account can modify the BIOS—ie toggle the wifi card. The regular account is used only to view the BIOS settings. The affiant deceitfully declined to adequately explain this critical difference, and that the government had previously configured the administrator account—the only account that can actually make any changes to the BIOS. So, as an initial matter, even if the laptop had not been configured with a regular user password, anyone who turns on the laptop can choose to set a regular user password; creating such a password does not indicate that the BIOS has been modified in any way—only if the administrator password was changed and the BIOS log indicated that settings were changed—which, of course, neither occurred. The affiant does not explain this critical point. Indeed, the government's observations actually definitively prove that the BIOS was never modified: the government actually admits that "IT staff was able to log in to the BIOS and access the Windows operating system using an administrator password." Since the government set the administrator BIOS password and obviously did not tell this password to Mr. Schulte, any conceivable "hack" of the BIOS would require this password to be reset. Since this password was still the same password set by the government, then obviously nothing had changed since the time the government configured the laptop.

Moreover, the government lied when it claimed "the bootup BIOS login screen was for a user password." The BIOS does not have a login screen—it simply prompts the user for a password; the government types their administrator password to boot the laptop and Mr. Schulte types his unprivileged password to boot the laptop. Hence, the BIOS password prompt could not possibly indicate that "it was for a user account" or indicate any modification to the BIOS.

Furthermore, the government lied when it claimed a user password "was not created by IT staff." The government sets both an administrator and unprivileged password in the BIOS; the privileged password for the IT department and the unprivileged password for the defendant. What this does is ensures only the defendant (or government) can boot the laptop—so other inmates cannot access any critical or sealed discovery provided by the government.

Next, the final statement on point (iii) in the affidavit is a complete fabrication: "In order to create a user BIOS account, the administrator account likely would have to be accessed, indicating that Schulte was able to either crack or bypass the administrator password."

In reality, as already discussed, anyone who powers on the laptop can set the unprivileged account if no password is set — this does NOT require access to the ~~unprivileged account that has a password~~ BIOS account. And the reason is the unprivileged account is unprivileged — it cannot do anything. Access to this account accomplishes nothing. It also doesn't make sense that someone would hack the administrator account to setup an unprivileged account. Why? For what purpose? If someone were able to "hack" or "bypass" the BIOS administrator account, then they would use that account to change the BIOS settings — they would not setup an unprivileged account that cannot change the BIOS settings. Hence, not only is the government's statement a deliberate fabrication, but the exact opposite conclusion must be drawn — the existence and use of the unprivileged BIOS account clearly indicates that Mr. Schulte cannot access the privileged BIOS account — and hence, cannot modify the BIOS settings.

Finally, it must be noted that Mr. Schulte provided the laptop to the government to install printer drivers in the winter/spring of 2022 — yet the government made no objection to this unprivileged BIOS password at that time.

In summary, the entirety of t.iii is recklessly fabricated: the government omitted the distinction between the BIOS privileged account used to modify settings and the BIOS unprivileged account used to view settings; the fact that the government's privileged account still retained the same password meant that Mr. Schulte never could have accessed the privileged account; the BIOS does not display a login screen, but merely prompts for EITHER the privileged or unprivileged password (there are no users or account names); the unprivileged account had been setup for Mr. Schulte by the government to prevent anyone from viewing Mr. Schulte's sealed and highly sensitive discovery; even if that were not the case, if no unprivileged password is set, then anyone who boots the laptop can set a password — this does not require access to the privileged account since the unprivileged account cannot do anything except view the settings; and finally, regardless, it makes no sense to set a password on the unprivileged account if you have access to the privileged account — you would just use the privileged account — and hence, the existence and use of the unprivileged account clearly indicates that Mr. Schulte does not have access to the privileged account. The government's complete fabrication of t.iii in its affidavit clearly indicates the affiant's reckless disregard for the truth — if that were not readily apparent by this point.

P. 14

3. Encrypted Partition

In section t.V (p.14), the government asserts that the existence of an encrypted partition constitutes probable cause that a crime occurred. While the Police State obviously desires access to every byte of data in existance, the deprivation of data to the Police State does not constitute crime or evidence of a crime. The government failed to inform the Court that the small, 15GB encrypted partition was created by the built-in Windows feature Bitlocker, and that use of this feature was neither disabled nor forbidden by the government.

The government also failed to inform the Court that it frequently seized Mr. Schulte's laptop and rifled through his attorney-client privileged documents without a warrant (2019 - to "repair" it; 2020 - to "fix" battery; 2021 - to install "printer drivers") As a pro se criminal defendant as well as a plaintiff in many civil rights Complaints against the government, Mr. Schulte had a right and legitimate reason to encrypt his work product.

Moreover, the inclusion of this observation is too stale to be considered, particularly in light of the fact that the government complained about its existence to Judge Furman. Since probable cause must "exist as of the time of the search and not simply as of some time in the past," "the facts in an affidavit supporting a search warrant must be sufficiently close in time to the issuance of the warrant and the subsequent search conducted." United States v. Wagner, 989 F.2d 69, 75 (2d Cir. 1993). "The two critical factors in determining staleness are the age of the facts alleged and the nature of the conduct alleged to have violated the law." United States v. Raymonda, 780 F.3d 105, 114 (2d Cir. 2015) (internal quotation marks omitted). Additional relevant factors include the nature of the information forming the basis for probable cause, and the nature of the evidence being sought. United States v. McGrath, 622 F.2d 36, 41-42 (2d Cir. 1980).

Here, two months elapse between the observation and the warrant - plenty of time to delete the encrypted container particularly since trial ended and secrecy of trial strategy is no longer an issue. Furthermore, the government never alleges the encrypted partition is unlawful or a violation of laptop usage — and does not even request its removal or seek a warrant at the time of the observation. Put simply, Section t.V cannot contribute to probable cause in any way whatsoever.

4. Defense Exhibits at Trial

The government attempts to dictate how Mr. Schulte can or should conduct his own defense in section V of the affidavit (p.14). "Based on my participation in this investigation and prosecution, I am not aware of any purpose related to Schulte's defense preparation for trial that would require him to have access to the ability to draft and edit source code in connection with the presentation of his defense." This is absurdly false. Mr. Schulte's 2020 and 2022 trials were highly technical and the government produced source code in both classified and unclassified discovery. See unclassified search variant for GitHub. There were also numerous government exhibits with source code. "Source code" was mentioned no less than 73 times at trial. [redacted]. Indeed the government alleged Mr. Schulte stole source code from the CIA and released it to WikiLeaks—the entire trial was about source code. Accordingly, Mr. Schulte's case is highly technical and clearly involves source code and programs to interpret and view the code, such as Visual Studio—which the government failed to mention in its affidavit that the government itself provided this utility to Mr. Schulte for this very purpose.

Moreover, according to the records, the source code in question was adapted from Microsoft code manuals provided to Mr. Schulte in discovery and was only 7 total lines. See, eg. Proposed Defense Exhibits 1210 and 1211; Tr. 934. There is no indication that Mr. Schulte himself built the binary executables or that this was performed by defense technical experts, in the record. But this strategy was a legitimate defense objective that Ms. Shroff performed at the first trial in 2020, and that Mr. Schulte attempted to strengthen at this trial in 2022. The Court accepted the general strategy. See Tr. 940: "THE COURT: All right. I think what we're going to have to do is take it up as it comes, see what Mr. Schulte tries to do with it, mindful of the limitations on what he can and cannot offer. I'm not sure the code, depending on how he uses it, it may not be offered for the truth per se, in which case I'm not sure there's a hearsay problem. But we'll take it as it comes, I guess." The purpose was to undermine the government's reliance of access file times at trial by introducing to the jury the fact that these times are easily changed, and should not be relied upon on their face.

Finally, even if Mr. Schulte could write and compile code, including malware, this does not in any way jeopardize the security of the laptop — viz the BIOS; there was no possible way to penetrate or crack the BIOS.

As an initial matter, the existence of Visual Studio does not mean it contained a compiler to build executables — Visual Studio can be installed, and indeed exists, independently of any compiler — particularly to parse, interpret and display source code to the user, for example, to review discovery. The government provides no evidence that Mr. Schulte personally built binaries on his discovery laptop or that the laptop ever had this ability.

Second, the government fails to note to the Court that Mr. Schulte has full Administrator access to his discovery laptop — and neither any reason nor any benefit to write malware to "manipulate" it. Any function that malware could perform, Mr. Schulte had the direct ability to do as an administrator.

However, this does NOT extend to the BIOS. Mr. Schulte is an administrator of the Microsoft Windows OS installed on the hard drive — but no ability to manipulate the BIOS. As already explained, the BIOS is essentially an independent operating system that runs on boot, but terminates once it passes control to the hard-drive installed operating system. And as previously discussed, Mr. Schulte did NOT have an administrator account in the BIOS - only View permissions. But of course, once control passes from the BIOS to Windows, whenever the BIOS is no longer running — and therefore no way for Windows to modify or interact with the BIOS; not even a Windows administrator or Windows malware. The BIOS and Windows are completely separate systems with no overlapped privileges. The affiant deliberately omits these crucial facts, and instead, absurdly alludes to the possibility of malware "modifying the operating" "manipulating" the device, implying — falsely — to the judge that Windows can manipulate the BIOS, which it cannot.

Finally, it must be noted that the BIOS [redacted] is not Windows, so any Windows-developed malware cannot effect the BIOS. An attacker would not need a completely separate program to write BIOS malware (which Mr. Schulte did not have), which would have to execute before Windows booted; however, the laptop was securely configured by the government for "Secure boot", preventing Mr. Schulte or any would-be attacker from doing so. See Laptop manual. Accordingly, it was never possible for Mr. Schulte to manipulate the BIOS, with or without a compiler to build Windows code.

P. 17

5. Remaining "Probable Cause"

Thus far we have examined the probable cause from ¶¶ 12-15), "Schulte's Manipulation of His Discovery Laptop." The remaining pages 3-12 do not establish probable cause; this section is in essence a compilation of every allegation the government has ever had against Mr. Schulte and why they believe he is Satan incarnate. It covers allegations from 2016 and 2018. The government also references the testimony of jailhouse snitch Carlos Luna Betances — but he was utterly destroyed on cross examination as a blatant liar and fraud; See e.g. Tr. 1760-1811. The jury did not credit any of his testimony. The remaining rant by the affiant contained a combination of evidence taken out of context, false conclusions, and wild theories that were rejected by the first jury in 2020. Although Mr. Schulte was convicted in 2022, it is still pending Rule 29 dismissal and not yet final. Moreover, if a prior arrest or conviction and government hatred were all that was needed to obtain a search warrant, then truly the Fourth Amendment would not exist.

Specifically, the government needed to provide the Court with contemporaneous facts about the alleged crime and link this to the items to be seized. The government does not even attempt to do this until page 12; and as we have shown, all of these "facts" are provably false. The government violated the scope of the hard drive swap and executed a warrantless search on 6/3/22; The affiant blatantly falsified evidence, fabricated evidence, and perpetrated a fraud upon the Court when it claimed in ¶ iv that the government did not know the status of the BIOS configuration despite clear transcripts to the contrary; the affiant fabricated ¶ iii with respect to BIOS access controls, falsely claiming that a BIOS login screen was for a user account, falsely claiming the unprivileged account was not setup by the government, and falsely asserting that access to the privileged BIOS account was necessary to set a password for the unprivileged account while in reality the fact that the privileged BIOS password was uncharged and the use of the unprivileged account by Mr. Schulte both proved that Mr. Schulte could not, and did not access the BIOS privileged account; finally, everything about the BIOS was irrelevant since the government physically disconnected the wifi adapter in the laptop.

The fraud committed by the government is both despicable and incorigible. The government has shown that it has absolutely no respect for the law or this Court — nor any respect for the trust and deference the Court shows the government when entertaining search warrants. The government believes itself above the law — that it can fabricate and falsify evidence with impunity. This Court is compelled by the Constitution to condemn the government's actions and grant this MOTION

P. 18 B. Unlawful Conversion of the July 26th Search Warrant into a General Warrant

In the alternative, if the Court upholds the July 26th warrant, it must nonetheless declare the ~~execution~~ conversion of that warrant into a general warrant unconstitutional and order the laptop returned or the search parameters severely restricted to the probable cause upon which the warrant was based — throwing out and disregarding ~~daily~~ ~~[illegible]~~ anything discovered beyond the original scope.

The chief evil that prompted the framing and adoption of the Fourth Amendment was the "indiscriminate searches and seizures" conducted by the British "under the authority of 'general warrants.'" Payton v. New York, 445 U.S. 573, 583 (1980); Arizona v. Gant, 556 U.S. 332, 345 (2009) ("[T]he central concern underlying the Fourth Amendment [is] the concern about giving police officers unbridled discretion to rummage at will among a person's private effects"). To prevent such "general, exploratory rummaging in a person's belongings" and the attendant privacy violations, Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971), the Fourth Amendment provides that "a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." Kentucky v. King, 131 S. Ct. 1849, 1856 (2011).

"Where, as here, the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance. As numerous courts and commentators have observed, advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain. There is, thus 'a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.' This threat demands a 'heightened sensitivity to the particularity requirement in the context of digital searches.'" United States v. Galpin, 720 F.3d 436, 446-447 (2d Cir. 2013) (citation omitted).

Thus, in the event the Court finds the July 26th warrant constitutional, the search is extremely limited to the paltry probable cause established: the "potential" modification of the BTOS. The warrant does not give the authority of a general warrant. The government must be restricted to the review of the BTOS only — if the BTOS was never modified, as is the case, then there is absolutely no reason nor permission to expand to review Mr. Schulte's files; if the BTOS was never modified and the wifi never enabled, then it is not possible that either of the two crimes

P.19 described in the warrant were committed. The search must end. Since the particular allegations here involved the wifi capability, the government's search must be limited to this single component. First and foremost, the government must check the connection between the wifi card and the motherboard — if this connection is still severed then no further search is authorized since the physical disconnection indicates it was impossible to use the wifi card. If this was re-soldered, then the government would be authorized to search the BIOS — but if the password for the privileged account was unchanged and the logs showed the wifi card was never enabled then no further search is authorized since this indicates it was impossible to use the wifi card. If this BIOS was modified, then the government would be authorized to search the Microsoft Windows system files to determine if the computer was ever connected to the internet, and so forth.

Yet this is not what the government did. The government knew that Mr. Schulte never connected the laptop to the internet, but simply used the courts to harass and intimidate him; the government simply executed a general warrant to hunt for evidence of any crime for which it could prosecute him.

Since the wifi card was never re-soldered, the search should have ended there. Since the privileged BIOS password was never changed ~~now~~ and the logs showed the wifi adapter was never enabled, the search absolutely should have ended there. Based on the "probable cause" and state of the laptop, this search should have ended within a day — and there was absolutely no reason for the government to go hunting through Mr. Schulte's files considering the government knew or should have known it was impossible for Mr. Schulte to use the wifi card and hence impossible to commit the crimes alleged on the face of the warrant.

Accordingly, this court should find the government's unlawful conversion of the July 26th search warrant into a general warrant and subsequent expansion of the search well beyond the bounds established by the probable cause as unconstitutional; the laptop must be immediately returned.

P. 20 C. The October 4, 2022 MDC Search was Unconstitutional

1. Fruit of the poisonous tree

Since the July 26, 2022 laptop seizure was unconstitutional (A) or the expansion and execution of that warrant as a general warrant to search every byte of data on the laptop for evidence of any crime well exceeded the probable cause upon which the warrant was based (B: i.e. the BIOS), and because the October 4, 2022 warrant is based solely on the evidence unlawfully obtained as a result of the unconstitutional search, then the October 4, 2022 is incontrovertibly fruit of the poisonous tree and therefore unconstitutional itself.

2. The alleged "child pornography"

a. Searching pictures and videos well outside established probable cause

In the event the Court upholds the July 26, 2022 search warrant the October 4, 2022 warrant is still unconstitutional as there was absolutely no probable cause to search Mr. Schulte's files on the laptop, much less pictures and videos. Assuming that the first search is lawful it only speculates that Mr. Schulte may have modified the BIOS to enable the wifi adapter; this is easily checked in 5-minutes time be reviewing the BIOS settings and logs. Once the government confirmed that Mr. Schulte did not, and could not have possibly modified the BIOS, the search is over—Mr. Schulte did not, and could not have possibly connected to the internet with a disabled wifi card. At the very most, the government could have checked the Windows logs to determine if or when the laptop was ever connected to the internet—another 5 minute check. After reviewing the Windows system files—not Mr. Schulte's personal files—and confirming that the laptop was never connected to the internet, then the search must end. That the government kept expanding the warrant is proof of the execution of a general warrant. Moreover, there was absolutely no reason whatsoever to review Mr. Schulte's personal files—particularly pictures and videos—as these cannot possibly be relevant when the laptop had a disabled wifi card and was never connected to the internet.

b. The alleged "child pornography" is actually adult pornography provided by the govt.

Finally, the only pornography on the laptop was adult pornography provided by the government pursuant to Fed. R. Crim. P. 16; they are files from public, mainstream download websites like, pornhub.com. They are not even close to child pornography.

3. Beyond the Scope of the Warrant

a. Seizure of three hard drives unlawful

The warrant particularly describes the subject premises "as Cell 80[illegible], Unit 4B4, located in..." MDC. However, the government unlawfully expanded that search to include the law library and office—which were not particularly described in the warrant. Specifically, after the warrant was executed, the agents left cell 80[illegible], went into the law library and seized two hard drives, then went into the office and seized a third hard drive. Indeed, the receipt only identifies "one WD Elements Drive." See Ex. D. But 4 drives were seized. Thus, in addition to violating the particularity requirement, the government also violated Fed. R. Crim. P. 41(f)(1)(C) by not providing Mr. Schulte with a receipt of the three additional stolen drives.

Since the government searched beyond the limits of the search described in its warrant, the seizure of the three additional drives is unconstitutional, and they must be returned. In an oft-quoted passage, the Supreme Court has held that the particularity requirement "makes general searches... impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." Marron v. United States, 275 U.S. 192, 196 (1927). Accordingly the three drives must be returned pursuant to Fed. R. Crim. P. 41(g).

b. Seizure of notebooks and paper documents

The government seized numerous notebooks and paper documents, but the October warrant did not establish probable cause to search paper documents—nor did it even proffer evidence that Mr. Schulte possessed paper documents. A search warrant must specify the "items to be [seized] by their relation to designated crimes." U.S. v. Williams, 592 F.3d 511, 519 (4th Cir. 2010); see also U.S. v. Buck, 813 F.2d 588, 590-92 (2d Cir. 1987) (finding that a warrant authorizing the seizure of "any papers, things, or property of any kind relating to [the] previously described crime" failed the particularization requirement because it only described the crimes—and gave no "limitation whatsoever on the kind of evidence sought."). "[A]n otherwise unobjectionable description of the object to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based." United States v. Galpin, 720 F.3d at 446. The government did not even proffer evidence that Mr. Schulte possessed notebooks, much less that they would contain evidence of a crime. The notebooks/papers must be returned.

IV. CONCLUSION

Every year the government fabricates some pretense to seize and search Mr. Schulte's laptop for no reason other than to screw with him and deprive him of his discovery. Every year the government seizes his laptop they copy all of his privileged work product including evidence and strategy in ongoing civil suits against the government. Frustrated by this unconscionable tactic, Mr. Schulte encrypted all his work product. When the government tried their despicable tactic again using the June 3rd hard drive swap as a pretense to copy Mr. Schulte's work product before trial to ensure strategic dominance, and in complete violation of the limited scope authorized by Mr. Schulte, lo and behold, the government found Mr. Schulte's work product encrypted! How dare he defend against our illegal tactic!

So the government falsified evidence, fabricated evidence, and perpetrated a fraud on the Court to seize the laptop in retaliation. The government ensured the laptop was compliant before returning it on June 3rd as the record indicates, but they lied anyway — because who will stop them? The government gets what it wants and does as it pleases with complete disregard and reckless abandon of the law — the government believes itself above the law; it has no respect for this Court and knows it can violate the Constitution with impunity.

The government is now wielding the law as a vindictive force to get what it wants — access to Mr. Schulte's privileged files. Until then, it will hold all of Mr. Schulte's work product hostage and deny him access to his discovery. There will be no prosecutions in this district for any criminal misconduct as the government knows Mr. Schulte commit no crimes, and they would be subject to Brady disclosures and other legal avenues for Mr. Schulte to adequately litigate and receive justice. But in the case where the government seizes property and does not prosecute, it achieves a form of immunity and can hold the property indefinitely.

Luckily, this form of tyranny and oppression was foreseen and Rule 41(g) provided as a civil equitable proceeding to counter this legal limbo. Accordingly, this Court should find the government's actions reprehensible and repugnant to society. This Court should not allow the government to commit outright fraud, perjury, and obstruction with impunity. No one else can or will hold the govt accountable for its actions. In the name of the Constitution, I hereby implore this Court to grant this motion.

Dated: January 14, 2023
Brooklyn, New York

Respectfully Submitted,
Josh Schulte

EXHIBIT A

June 3, 2022 CIPA Transcript
in U.S. v. Schulte, 17 CR 548 (JMF)
Pages 110-113; 173-180; 197-199

THE COURT: All right. I'll pick up where we left off, but in closed classified session.

MR. HARTENSTINE: Sorry, your Honor.

THE COURT: We're good?

MR. HARTENSTINE: Your Honor, yes. Everyone who is in attendance are appropriately cleared and the courtroom has been secured for classified discussion.

THE COURT: OK. Everybody please just keep your voices up so that the court reporter can hear. Hopefully we can make it work even with masks, which is technically what our protocols require. If not, we'll figure it out what to do.

MR. DENTON: Your Honor, real quickly before we begin, in the interest of time, we just wanted to briefly have a conversation on the record that the U.S. Attorney's office is going to take possession of the defendant's broken laptop in the interest of trying to have our IT staff execute this hard drive swap with the replacement as soon as it's available.

We just wanted to make sure there was some record the defendant was aware of it and consented to us doing that.

THE COURT: OK. I'm guessing his consent may be contingent on this. I assume it goes without saying that the contents would not be viewed by anyone, but certainly not by anyone associated with the trial team in any way, shape, or form?

MR. DENTON: Only the IT staff as necessary to assure

accomplishment of the objective.

THE COURT: OK. Mr. Schulte?

THE DEFENDANT: IT staff should not talk to him, but yes.

THE COURT: I think that was implicit in what Mr. Denton was saying.

Just to make it explicit, I take it, Mr. Denton, you would represent that no one on the trial team will know anything one way or another about the contents of the laptop, other than the mere fact that it did or didn't work to transfer?

MR. DENTON: Certainly not, your Honor.

THE COURT: Mr. Schulte, with that understanding?

THE DEFENDANT: Yes.

MR. LOCKARD: One additional clarification. They said they may need the log-in information in order to make the transfer happen or swap the hard drives. So, Mr. Denton and I don't need the log-in information. Our IT staff would like the log-in information so they can do this.

THE DEFENDANT: I'll authorize standby counsel, if needed. I don't think it shouldn't be needed for swapping the stuff. If so, standby counsel can speak with them and give it to them.

MR. LOCKARD: We're going to try to to this, this afternoon. I don't know how long this conference is going to

go, but we're going to try to do it this afternoon. If it runs too late, we may lose access to the personnel who would be able to do it today.

THE COURT: OK. Well, all the more reason, let's get started and try to do this as swiftly as we can. I'm sure you all want to be done with this as, as I want to be done with this. I didn't think we would be going this long as it is.

One other option on that front would be for Mr. Schulte to write down the log-in information and put it in a sealed envelope, and that would be provided to the IT staff only to be used in connection with the swap. That might facilitate things and avoid any miscommunication.

MS. SCHROFF: That's what we did the last time, your Honor. We're prepared to do it again. This is not an issue. I don't know why --

MR. LOCKARD: Cheryl is requesting to take the broken laptop back now.

Do you want to give her the log-in information?

MS. SHROFF: Sure. We offered that to you when we gave it at one o'clock.

THE COURT: Write that down now.

Ms. Smallman, do we have an envelope?

Does someone have an envelope?

(Pause)

Let's get started then. Various issues on my agenda

are the most recent Section 5 notice that Mr. Schulte filed, I think, yesterday, maybe a date from a few days ago. In any event, I got it yesterday, his letter dated yesterday raising three items. One pertaining to the [redacted] substitution issue, one relate to the use of pseudonyms, and the third the information issue.

The third, if we have time to get there, would be the 6E motion on NDI. We also need to discuss further the audio recordings that we began discussing upstairs.

I don't know if others have additional items? I think that covers -- oh, and the witness list issue as well.

Let's start with the witness list issue. Again, I think both sides have a point here. I don't know if there is an amicable way of just cutting through this and resolving it, but it does seem to me like the government's arguments are most forceful with respect to [redacted] as to whom bringing them here would be rather burdensome.

Mr. Schulte, I'm not saying you're proceeding in bad faith. I think to the extent that it can be identified ahead of time that you don't intend to call someone, obviously bringing them here just for the sake of bringing them here is not something I want to entertain or license, and to the extent that we can resolve any legal issue before they are brought here, we should.

up.

This not just one exhibit. This is all the MCC counts. I know there is countless exhibits through the CIPA 5. There is at least 20 different exhibits that we're going to be going through. And depending on how the government is bringing this up through each witness, could be brought up through every single witness, too.

This is a substantial closure, and I'm just not able to make this same argument that this information is not national defense information. Look at it, it's just being able to talk openly to the witness so that the jury can see. It's just way too -- it's way too prejudicial to do that.

If you're looking at the reasons for it, I mean, most of the time, this type of information is information that if you're going to do a courtroom closure, it's to protect identities of actual undercover assets or something like this. Where the information is already on the Internet, the question then becomes, when can the government not close the courtroom.

I mean, why can't they just close the courtroom for every single thing that they say is classified and introduce it all through this supposed CIPA 8 loophole, closing the courtroom, information already on the Internet can't even be introduced in the courtroom, then that just opens the door to everything.

I mean, why do we even have the first CIPA hearing?

A-6

Why not introduce all those as classified, too, right? It's a slippery slope, doesn't make any sense, and there is clear prejudice and very little harm to the government. This stuff is already on the Internet. [redacted] [redacted] There is simply no harm. The DevLAN network is offline. These tools aren't being used. There is no harm.

THE COURT: I got it.

I think the court reporter needs a break and it is hard to do her job. I want to respect that. So let's take a ten-minute break, and then we'll pick up from there. Obviously, I would like to finish this up as quickly as we can, but we need to work through some of these issues.

I'll see you in ten minutes.

(Recess)

All right. Thank you.

Let me just apologize to the court reporter. I'm not sure she reasonably expected this would be an all-day matter. I certainly didn't. I appreciate everyone's patience.

With that, yes, Mr. Lockard.

MR. LOCKARD: Your Honor, in the interest of continuing to address things that we didn't expect to address, I did want to provide an update about the laptop and pose a request to Mr. Schulte.

So the update is that our IT staff was able to power

up the computer. It did boot up. They are unable to log in to check to see if the hard drive is working. The password they received did not work.

So the request from Mr. Schulte is, can we get the correct password for the laptop. The second part of the update is that when the IT personnel did boot the computer up, it appeared to them that the bios configuration had been changed. The bios configuration, my understanding that that is the system that runs the hardware and the ports and things like that, in way that they can no longer confirm if the laptop is compliant with BOP and DOJ security requirements.

So if we do get the correct passwords, they will be able to confirm or reset the security settings so that the laptop can go back to the MDC with Mr. Schulte.

THE COURT: The suggestion being that Mr. Schulte altered the bios settings, whatever that may be?

MR. LOCKARD: Your Honor, we are making no inferences. He's had the laptop a long time. They would like to reconfirm the configuration.

THE DEFENDANT: The laptop is working now? Hold on.

(Defense confers)

THE COURT: First item is, I think we need to give the government the correct password so the IT folks can see if they can get to the content. I thought that had been done.

THE DEFENDANT: I gave them -- I mean, I gave standby

A-8

counsel the correct password. To the degree they are not working...

To confirm, they are able to get the laptop itself powered on and working, or they just took the hard drive out or what were they able to do to fix the laptop?

MR. LOCKARD: They were able to turn the laptop on. It did boot up. The password you provided could not -- did not provide access to the laptop.

THE DEFENDANT: Could it have been reset somehow, factory reset or something?

Is there any way, after this is over, that they can bring the laptop, and standby counsel and myself can look through it to see if it's been reset, or if is that acceptable?

MR. LOCKARD: I don't know the answer to any of those questions. This is what I have been conveyed. I think in light of the concern about the configuration settings, our IT needs to make sure that it is still configured appropriately for being able to be in BOP space and used by an inmate.

THE DEFENDANT: The laptop has been provided to them before and hasn't been changed since the last time the government reviewed it. Nothing has changed since then.

To the degree anything is different, I don't know. It could be a reset, if the laptop could have been reset or something.

It just would be nice if standby counsel and myself to

be able to -- if it's been reset, that would explain why the passwords don't work anymore, right? That's all I'm trying to figure out.

(Defense confers)

MR. LOCKARD: OK.

THE COURT: I don't know what to tell you.

MR. LOCKARD: This is where you are. If you can provide us with passwords that work --

MS. SCHROFF: Can you give him the password back?

MR. LOCKARD: We don't have it.

THE COURT: Guys, I don't know why you couldn't have discussed this before I came out.

In any event, Mr. Schulte, write the password down again, give it to Mr. Lockard, and they will try that. Maybe it a handwriting issue. I don't know.

I certainly agree, if the bios configuration is not what BOP and protective order requires, then that should be conformed to what it does require, without intimating who did what. Bottom line is, first step is to get access to the computer. Hopefully we can resolve it here now.

MR. LOCKARD: Yes.

Our goal is to make sure it is compliant, get it fixed, back to Mr. Schulte. If he writes down the password, I'll hand it back to the paralegal to take to the IT department.

MS. SCHROFF: We did try to resolve it before the court came out, your Honor. The government wanted it on the record.

THE COURT: Since we're not going to be together again until Wednesday, what happens if this doesn't work?

What's the backup plan?

MR. LOCKARD: I don't know. Mr. Schulte does have a SCIF day Monday and potentially Tuesday. We may be able to discuss it with him on Monday, or see whether IT staff comes back, after they have a chance to take a second look at it. Beyond that, I don't know.

THE DEFENDANT: My question is, if the laptop is working, why can't they just -- I brought it here through the marshals. Why can't they just bring it here and have standby counsel and myself look through it, and if it is working, then we can just take it back and I can continue working on the case?

THE COURT: You can't take it back if it's not configured according to --

THE DEFENDANT: We'll look through and sit with the IT people.

THE COURT: Bottom line is, try to work this out as fast as you guys can. Government has an incentive to do that. If this lingers, the likelihood of adjournment goes up. I imagine the government is not eager for an adjournment. I'm

not eager for an adjournment. So see if you can sort it out today, and if you can't sort it out today, I urge you to try to figure it out over the weekend on Monday. In any event, the sooner, the better. I'll deal with whatever comes, if it isn't resolved by Wednesday, we'll have to do what we have to do.

I did speak to the U.S. Marshal, by the way, and he seemed to think it would not be a problem to arrange an extra SCIF day on Tuesday. He was probably leaving me a message as I'm sitting here. I don't know the answer. I'm hoping that means Mr. Schulte gets an extra SCIF day on Tuesday.

Back to the NDI issue, Mr. Denton, let me turn to you and ask you two things: One is, first of all, if this is a proper approach, whether it is analyzed as a CIPA issue or *Waller* issue, what have you, why doesn't Section 8 swallow Section 6C whole?

That is to say, under what circumstances is it appropriate to do this, as opposed to going through the 6C process and either requiring new classification or providing the government an opportunity to make substitution or redaction?

Why wouldn't this always be the way it's done? That is one question.

The second is, you use [redacted] as a specific example. Maybe it would be helpful to talk through how Mr. Schulte can make the arguments he wants to make with

A-12

that as a specific example. I think to complicate matters further, what I understand the case may be is that Mr. Schulte intends to or wants to introduce articles from newspapers and elsewhere [redacted] and basically say, Look, see my disclosure from the MCC. That was already public. See this *New York Times* article, and it doesn't matter.

How would that happen and work at trial?

MR. DENTON: Your Honor, I think to take those in order, first, Section 8 does not swallow Section 6 for a number of reasons. First is, as explained by Judge Ellis and the court and various others, we do not have star chamber trials in which everything is classified. Section 8 obviously runs into some limits at some point. One of those is practical, which is that both parties do want to be able to exhibit exhibits, and so there is a volume consideration that it is appropriate for certain things at a certain level of sensitivity and a certain practicality in handling them. And Section 6 is appropriate for, frankly, the vast majority of everything else.

This is appropriate in this situation because, for reasons that we have laid out previously, redacting these documents is a unique challenge. so the Section 6 process is not particularly well-suited to this type of information.

For that reason, I actually think it makes sense to table the question of [redacted], because if we were just talking about the classified leak

sense that, by the time the defendant testifies, I assume he would probably testify last as part of a defense case. The reasons to keep those things ex parte may no longer be applicable in which case. There may be no justification to keep them ex parte, and the government would get them.

But separate and apart from that, you're completely right. You may be entitled to some prior relevant statements, and I'll certainly consider that. You should raise it in the appropriate time.

MR. DENTON: Just flagging it now, not something that needs to be resolved.

THE COURT: OK. Understood.

Anything else from the government?

MR. DENTON: No, your Honor.

THE COURT: Mr. Schulte?

THE DEFENDANT: No, I don't think so, except for the laptop. Is there -- I don't know if the court is able to have issue an order or something for me to be able to remain here for another 15 or 20 minutes to try to resolve it before I have to go back.

THE COURT: Is it possible to find out whether and when it would be we would have an answer?

You don't have your phone in here. Is that possible to find out?

MR. LOCKARD: It's going to be the first thing we

attend to after the conference is over.

THE COURT: Do the marshals know timing in terms of Mr. Schulte's return to the MDC?

MARSHAL: We're ready for immediate departure.

THE COURT: I'm sure. If you need a delay, it is what it is. I, too, am ready for immediate departure.

I think it would make a lot of sense to hold off for 15 minutes to at least find out if there is a resolution. If there is a resolution, then it may be as simple as telling Mr. Schulte that, and then he can go back.

If there isn't, I don't know the best way to approach this. Seems like the government get an answer, make sure Mr. Schulte knows where things stand, and then he can go back at that point.

Does that make sense?

MR. HARTENSTINE: Your Honor, if I might suggest, if we call an end to the classified discussion, then everyone could have their cell phones back and perhaps look into this issue.

THE COURT: Even better.

I'll stay on the bench. Go get your phone and let's try to get an answer.

MS. SCHROFF: Your Honor, may I ask on Wednesday, if there is a time for the court appearance?

Ms. Colson and I are both traveling Tuesday and not

sure when.

THE COURT: I think I said 9:15. I don't have the docket here. I'm pretty sure I said 9:15. The only thing I will give you heads up about, I have another appearance at 11, maybe ones after that. I don't have my calendar with me. It's on my phone.

Given how long this went and given the potential need for a classified session next Wednesday, I may -- I don't know -- just plan to have Wednesday open for whatever we need to do. We'll have to work around things as best as possible.

Starts 9:15.

MS. SCHROFF: I just ask because we have the witnesses the day before, not in New York. I want to make sure I can go back.

THE COURT: The order said 9:15.

I'll stay here and hopefully get good news in a moment.

(Adjourned)

EXHIBIT B

The Unconstitutional 7/27/22 Search warrant

B-1

TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

APPLICATION FOR LEAVE
TO FILE DOCUMENT UNDER SEAL

****
In the Matter of the Application of the United States of America for a Search Warrant for an Asus Laptop Model Expert Book B9450 currently held

22-MJ-798
Docket Number

****

SUBMITTED BY: Plaintiff___ Defendant___ DOJ ✓
Name: Joshua B. Dugan
Firm Name: USAO-EDNY
Address: 271 Cadman Plaza
Brooklyn, NY
Phone Number: 718-254-6144
E-Mail Address: joshua.dugan@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES___ NO ✓
If yes, state description of document to be entered on docket sheet:

A) If pursuant to a prior Court Order:
Docket Number of Case in Which Entered:
Judge/Magistrate Judge:
Date Entered:

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

Ongoing criminal investigation

ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE, AND MAY NOT BE UNSEALED UNLESS ORDERED BY THE COURT.

DATED: Brooklyn, NEW YORK
7/27/22

U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE
DATE

MANDATORY CERTIFICATION OF SERVICE:
A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, B.) ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation:_____; or C.) ✓ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

July 26, 2022
DATE

SIGNATURE

USG-CONFIDENTIAL

USAO_JAS_028210

B-2

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States of America for a Search Warrant for an Asus Laptop Model Expert Book B9450 currently held at the Metropolitan Detention Center.	**TO BE FILED UNDER SEAL** **Agent Affidavit in Support of Application for Search and Seizure Warrant** 22-MJ-798

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, SEAN COLLINS, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been so employed since 2019. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. Since approximately February 2020, I have been assigned to the FBI's New York Field Office, Counterintelligence Division. During my tenure with the FBI, I have participated in counterespionage and counterintelligence investigations and, among other things, have conducted or participated in surveillance, the execution of search warrants, and the review of stored electronic information for evidence of crime. Through my experiences in the field and training relating to counterespionage and counterintelligence and related crimes, I am familiar with some of the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United States by misusing their access to classified and national defense information. I am also familiar,

B-3

though my training and experience, with the use of cellphones and computers in criminal activity and the forensic analysis of electronically stored information.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search an Asus laptop model Expert Book B9450 (the "**Subject Device**") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Device

3. The **Subject Device** is particularly described as an Asus laptop, model Expert Book B9450. The **Subject Device** was provided to Joshua Adam Schulte, a federal inmate, in or about July 2021 in connection with his review of discovery pursuant to Rule 16 of the Federal Rules of Criminal Procedure. The **Subject Device** was provided by Schulte's then-counsel, the Federal Defenders of New York, to the U.S. Attorney's Office for the Southern District of New York for a security review. The **Subject Device** was then provided to the Metropolitan Correctional Center ("MCC"), where Schulte was housed at the time. Schulte is currently detained at the Metropolitan Detention Center ("MDC").

4. Based on my training, experience, and research, I know that the **Subject Device** has external ports that permit it to connect to external devices, including Universal Serial

B-4

Bus ("USB") ports. These ports allow the Subject Device to connect to USB devices such as thumb drives and external disc drives. The Subject Device also has WiFi capability that allows it to connect to wireless networking technology. If enabled, WiFi capability could permit the Subject Device to connect to an available wireless network or, if the user of the Subject Device has access to a cellphone with "hotspot" functionality, to a cellular network. I have learned that, as part of the security review conducted by the U.S. Attorney's Office prior to providing the Subject Device to the MCC, the Subject Device was "air gapped," that is, its wireless capability was disabled.

C. The Subject Offenses

5. I respectfully submit that probable cause exists to believe that the Subject Device contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 401(3) (contempt of court) and 1791(a) (possessing contraband in a correctional facility), as well as conspiracies and attempts to violate these provisions and aiding and abetting these offenses (the "Subject Offenses").

II. PROBABLE CAUSE

A. Probable Cause Regarding Commission of Subject Offenses

6. This application is in connection with the investigation of Joshua Adam Schulte for crimes arising out of his theft of classified, national defense information from the Central Intelligence Agency ("CIA") in 2016 and transmission of that stolen classified information (the "Classified Information") to WikiLeaks.org ("WikiLeaks"); his obstruction of the investigation of those offenses in 2017; and his unlawful transmission and attempted transmission of additional national defense information to a reporter and the public from prison in 2018. Since 2021, I have been involved in the investigation of those offenses as well as the trial of those offenses beginning on June 13, 2022. *See United States v. Schulte*, S3 17 Cr. 548

B-5

(JMF) (S.D.N.Y.). I have, among other things, reviewed prior applications for search warrants issued in connection with this investigation and records of court proceedings, and have spoken with information technology ("IT") staff at the U.S. Attorney's Office. I have learned the following:

Schulte's 2018 Violations of a Protective Order and Unlawful Use of Contraband Cellphones in Prison

a. In 2016, Schulte was employed by the CIA as a computer software developer. Schulte worked in the CIA's Center for Cyber Intelligence ("CCI"), which was responsible for the CIA's offensive cyber operations. Specifically, Schulte worked in the Engineering and Development Group ("EDG"), which produced computer programs, also known as "cyber tools," that other CIA components used in foreign intelligence cyber operations to collect intelligence from foreign adversaries and terrorist organizations. Schulte and other developers in EDG used a closed, classified CIA computer network, called DEVLAN, to develop and test these foreign intelligence cyber tools. On or about April 20, 2016, Schulte accessed a network location on DEVLAN where backups of certain development tools used by EDG were stored and copied a set of backup files (the "Backup Files"). The Backup Files contained information about essentially all cyber tools developed or in development by EDG, including source code and documentation. Schulte later transmitted the Backup Files to WikiLeaks, which began releasing information from the Backup Files on its website on March 7, 2017. WikiLeaks continued to release data from the Backup Files on several occasions throughout 2017. WikiLeaks dubbed these releases "Vault 7" and "Vault 8." Schulte left the CIA in November 2016, after which he moved to New York, New York.

b. On or about March 15, 2017, the FBI executed a warrant to search Schulte's New York apartment. Among other things, a home computer was recovered as part of

B-6

that search. The home computer was later analyzed by FBI Computer Analysis Response Team ("CART") personnel and FBI computer scientists, who discovered multiple layers of encryption on parts of the hard drive. One encrypted partition was found to contain numerous images of child pornography.

c. On or about September 6, 2017, Schulte was charged in an indictment with crimes relating to the receipt, possession, and transportation of child pornography.

d. On or about September 18, 2017, a Protective Order was entered in the case (the "Protective Order") which, among other things, provided that certain materials designated by the Government as "USG-CONFIDENTIAL" could only be disclosed by Schulte to members of his defense team, including defense counsel, support staff, and expert witnesses.

e. Following his arrest, Schulte was initially released pending trial subject to bail conditions. On or about December 14, 2017, Schulte's bail status was revoked and he was ordered detained pending trial. At that time, Schulte was designated to the MCC.

f. On or about June 29 and 30, 2022, Carlos Betances Luna Mera testified at Schulte's trial. In his testimony, in sum and substance, Betances described Schulte's use of contraband cellphones in the MCC in 2018. Based on Betances' testimony, Schulte used, in particular, a contraband Samsung cellphone that Schulte equipped with a Virtual Private Network ("VPN") application, which conceals the user's Internet Protocol ("IP") address and, accordingly, the location from which the user accesses the internet; an application for anonymous internet browsing; and several encrypted email and messaging applications. Betances testified that, prior to using the contraband Samsung, Schulte had used a contraband iPhone. After the FBI seized a computer from a relative of Schulte's, Schulte became scared and

B-7

decided to replace the iPhone with the Samsung phone. Schulte claimed that he could change the IMEI ("International Mobile Equipment Identifier") number of a Samsung phone, which would have the effect of obscuring the identity of the phone and from where it was obtained. Furthermore, Betances described Schulte's unsuccessful efforts to obtain a USB drive, and another effort by Schulte and another inmate to have the contraband Samsung cellphone smuggled into the MCC law library, where inmates have access to computers for purposes of legal research, discovery review, and email access. From my training and experience and my participation in this investigation, I believe that Schulte's purpose in attempting to obtain a USB drive and his purpose in attempting to bring the contraband Samsung cellphone to the law library related to attempts to transmit discovery materials subject to the Protective Order outside of the MCC. I am aware that prisons typically make electronic discovery available to detained defendants in the prion law library and, as described below, Schulte (a) created handwritten notes at the MCC in September 2018 that appear to refer to providing discovery materials to WikiLeaks and (b) used an encrypted, anonymous email account created using the contraband cellphones to ask an associate to obtain a device capable of transferring data from a data storage location onto a cellphone or vice versa. See infra ¶ 6(l), (n).

g. Based on Betances' testimony, while at the MCC, Schulte said, in sum and substance, that, if he had a laptop computer, Schulte could "open the doors of the MCC." Schulte also said, in sum and substance, that the CIA had betrayed him and humiliated him.

h. On or about October 1, 2018, the Honorable Paul A. Crotty, United States District Judge, issued a warrant to search certain premises at the MCC (the "MCC Warrant") based on the application and affidavit of FBI Special Agent Jeffrey David Donaldson

B-8

(the "Donaldson Affidavit"), 18 Mag. 8377. As described in the Donaldson Affidavit, in or about April 2018, Schulte participated in a recorded telephone call from the MCC with an individual who appeared to be a reporter. During that call, in sum and substance, Schulte described certain information from search warrants that had been provided to him in discovery and described that the information was covered by a protective order. On or about May 15, 2018, the Washington Post and the New York Times published articles about Schulte's case in which they indicated that their reporters had learned of information in at least one of the search warrant affidavits provided to Schulte in discovery. On or about May 21, 2018, Judge Crotty held a conference during which Schulte was admonished about the provisions of the Protective Order and confirmed that he understood them.

i. On or about October 3, 2018, the FBI executed the MCC Warrant and recovered, among other things, notebooks (the "MCC Notebooks"), which MCC officials had removed from Schulte's cell prior to the execution of the warrant. On the outside of two notebooks was written "Attorney-Client Privileged." Later that day, Judge Crotty issued a second warrant to search the MCC Notebooks pursuant to wall review procedures, 18 Mag. 8442. Following the wall review, the MCC Notebooks were found to contain writings that appear to be draft Tweets intended for publication on Twitter, a social media platform. The notebook also contained handwritten notes relating to accounts with social media, email, and internet publication platforms. On a page titled "Tuesday 21st" (which, from context, appears to refer to August 21, 2018), Schulte wrote, among other things:

1) Delete all Google Docs from johnsmith
2) Delete all emails from johnsmith
3) Delete suspicious emails from my gmail
   a) New logons from phones
   b) Paypal
   c) Wordpress

B-10

Bartender. A CIA toolset for [operators] to configure for deployment." In a subsequent page, Schulte wrote another version of this apparent Tweet: "Let me first authenticate establish credibility myself [sic] . . . [@vendor] discovered [tool] in 2016, which is really the CIA's Bartender tool suite. [Redacted] Bartender was written [redacted] to deploy against various targets. The source code is available in the Vault 7 release." The CIA cyber tool Bartender has never been publicly identified with any malware discovered by commercial software or anti-virus vendors and has never been publicly associated with the tool described in the vendor report identified in Schulte's writings. Current CIA officers have described the adverse national defense impact of disclosing this information, including giving foreign adversaries the ability to identify CIA cyber operations that involved the use of Bartender, increasing the likelihood of foreign adversaries identifying related cyber operations, and the risk of exposing individuals involved in the deployment of the cyber tools on foreign computer networks.

k. On a subsequent page of the MCC Notebooks, Schulte wrote a draft Tweet or social media post addressed "To the United States Intelligence Community." The draft Tweet read, in part, "Your service, intense security investigations, and pristine criminal history can't even get you bail. As Josh Schulte has said, you are denied a presumption of innocence. Ironic, you do your country's dirty work but when your country accuses you of a crime you are arrested and presumed guilty. Until your country govt protects you and honors your service, send all your govt's secrets here: WikiLeaks."

l. On a subsequent page of the MCC Notebooks, dated "Wed. 9/12," Schulte wrote an apparent to-do list or schedule for editing and finalizing "copy," apparently

---

discovered. The vendor did not attribute the malware it identified to the CIA and did not use the CIA's project name "Bartender."

B-11

referring to various essays he had written for publication on Wordpress or to the draft Tweets, and for scheduling Tweets.2 One entry in the list or schedule read "Monday 17th – Tues 18th: DL Disc, UL WL." From my participation in the investigation, I believe this was shorthand for "download discovery, upload to WikiLeaks." I believe that this shorthand relates to Schulte's efforts, described by Betances, to obtain a USB drive and to smuggle the contraband Samsung into the MCC law library, where his electronic discovery was stored at the time.

m. Schulte, using the email account "annon1204@protonmail.com," exchanged emails with Shane Harris, a reporter for the Washington Post, who was using the email account "shanewharris@protonmail.com." In those emails, Schulte pretended to be an unnamed third person who was a friend of the Schulte family. On September 24, 2018, Schulte emailed Harris an electronic copy of a March 13, 2017 application for a warrant to search his apartment in New York, New York. Each page of the warrant was stamped "USG-CONFIDENTIAL," denoting that it was subject to the Protective Order and could not be disclosed outside Schulte's defense team. Schulte also included several pages of his own notes and commentary on the application, including notes with non-public information about the number of personnel in EDG and in a sister group, COG, which was the group that requested and deployed the cyber tools designed by EDG developers. Current and former CIA officers have described this type of information about CIA personnel to be classified and have described the advantages that public disclosure of the information would give to adversaries, including the ability to infer information about CIA intelligence resources and priorities, about types and locations of CIA cyber operations, and about locations and identities of CIA cyber personnel.

---

[2] Among other online accounts Schulte opened in approximately August and September 2018 was an account with Buffer, which is a service that allows users to schedule the release of social media posts in advance, including Tweets.

B-12

n. Schulte also used the "annon1204@protonmail.com" account to communicate with another email account hosted by Apple, Inc. (the "iCloud Account"). During one such communication in or about September 2018, Schulte requested that the individual using the iCloud Account purchase a specific electronic device (the "Device"). The Device is capable of transferring data from a data storage location onto a cellphone or vice versa. Based on my review of records obtained concerning the suspected user of the iCloud Account, I have learned, among other things, that the user of the iCloud Account later arranged for the purchase of a piece of equipment with capabilities similar to those of the Device.

o. As described above, the FBI searched the MCC on or about October 3, 2018, seizing Schulte's MCC Notebooks as well as the contraband Samsung and other contraband phones. Schulte was later placed on Special Administrative Measures ("SAMs") by the Attorney General pursuant to Title 28, Code of Federal Regulations, Part 501, later in October 2018, and has remained subject to SAMs since that time.

p. On or about March 9, 2020, Schulte was convicted following a jury trial of violations of 18 U.S.C. §§ 1001 (in connection with false statements Schulte made to the FBI during the investigation of the theft of the Classified Information) and 401(3) (in connection with Schulte's violation of the unclassified Protective Order entered in this case). On or about July 13, 2022, Schulte was convicted following a jury trial of violations of 18 U.S.C. §§ 793(b), 793(e), and 1030 (in connection with Schulte's theft and transmission of the Classified Information to WikiLeaks); 18 U.S.C. § 793(e) (in connection with Schulte's transmission of classified information to a Washington Post reporter while incarcerated at the MCC); 18 U.S.C. § 793(e) (in connection with Schulte's attempted dissemination of other

classified information while incarcerated at the MCC); and 18 U.S.C. § 1503 (in connection with Schulte's obstruction of the grand jury investigation of the theft of the Classified Information).

Schulte's Manipulation of His Discovery Laptop

q. In July 2021, Schulte was provided with the **Subject Device** as a replacement discovery laptop in order to review unclassified discovery pursuant to Rule 16 in jail. As described above, the **Subject Device** was procured by his former counsel, the Federal Defenders of New York, and provided to the MCC by the U.S. Attorney's Office following a security inspection and air-gapping.

r. In approximately October 2021, Schulte was moved to the MDC.

s. Through the discovery materials loaded onto the **Subject Device**, as well as additional external hard drives produced to him at the MCC and MDC, Schulte has had access to unclassified discovery materials in his prison cell. Schulte has had access to classified discovery and to the contents of his home computer, which contains child pornography, through regular visits to the courthouse Secured Compartmented Information Facility ("SCIF") where classified discovery is available to him and standby counsel, and where the child pornography discovery is stored in a safe. Schulte's visits to the SCIF are monitored by video by members of the U.S. Marshals Service and the FBI.

t. On or about June 1, 2022, standby counsel for Schulte sent a letter stating that the **Subject Device** was dropped by a guard at the MDC and was no longer functioning. On or about June 3, 2022, Schulte appeared in court for a pretrial conference, and brought the **Subject Device** from the MDC. At the request of Schulte and standby counsel, the **Subject Device** was delivered to IT staff at the U.S. Attorney's Office in order to determine if the **Subject Device** could be restored to functioning. Because of the possibility the Subject

B-14

Device contained attorney-client communications, attorney work product, or trial preparation materials, IT staff was instructed not to substantively review data on the **Subject Device**. I understand that, from a review of the **Subject Device**, IT learned the following:

i. The charging cable provided with the **Subject Device** was not the correct charging cable for that model of laptop. IT staff used a different charging cable that is compatible with the **Subject Device**, and the **Subject Device** could then be powered on.

ii. Upon powering on the **Subject Device**, a BIOS ("Basic Input/Output System") login screen was displayed. A computer's BIOS is software stored on a microprocessor that provides certain services for the operating system and initializes computer hardware during bootup. Modifications to the BIOS could potentially re-enable disabled hardware, including re-enabling WiFi connectivity. When the **Subject Device** was originally air-gapped, IT staff physically disconnected the wires connecting the WiFi from the motherboard of the **Subject Device**.

iii. The bootup BIOS login screen was for a user account, which was not created by IT staff when the **Subject Device** was initially inspected prior to providing it to the MCC. IT was able to log in to the BIOS and access the Windows operating system using an administrator password, but did not have access to the changed user password. In order to create a user BIOS account, the administrator account likely would have to be accessed, indicating that Schulte was able either to crack or to bypass the administrator password.

iv. In light of the instructions IT staff received about limiting review of the **Subject Device** to restoring operability, IT staff did not review whether BIOS

settings for the Subject Device had been changed or whether the wireless capability had been reconnected to the motherboard.

v. The hard drive of the Subject Device had a 15-gigabyte encrypted partition.

u. The U.S. Attorney's Office IT was able to restore the Subject Device to functionality by charging it with a new power cable. It appeared that the loss of function was due to a loss of power and not to any damage. The Subject Device was returned to Schulte along with a replacement power cable. Schulte was admonished about electronic security requirements, that he is not permitted to enable or use any wireless capabilities on the laptop, and that attempting to do so may result in the laptop being confiscated and other consequences.

v. On or about June 21, 2022, during the pendency of the jury trial in this matter, Schulte provided certain proposed defense exhibits to the Government. Among those exhibits were computer code that Schulte had written on the discovery laptop using the application-Visual Studio. Based on my training and experience, I know that Visual Studio is a Microsoft computer program that allows for the creation and editing of source code in a variety of different programming languages. Based on my participation in this investigation and prosecution, I am not aware of any purpose related to Schulte's preparation for trial that would require him to have access to the ability to draft and edit source code in connection with the presentation of his defense. In addition, Schulte provided the Government with the source code that he had written in the form of an executable file. Based on my training and experience, I know that the translation of source code from the text format used in a development environment such as Visual Studio requires the use of a "compiler," which is a separate computer program or

B-16

program extension that converts the source code text into a format that can actually be "run" on the computer as a program. Schulte provided these exhibits to the Government by burning them to a disc directly from the **Subject Device** using a CD/DVD rewritable drive that the Government temporarily provided him while present in the courtroom for that purpose. Accordingly, it appears that, although unnecessary for his preparation for trial, Schulte has acquired the ability to draft and compile source code for executable programs on the **Subject Device**, which would similarly allow him to draft and compile other programs, including malware, to manipulate the **Subject Device**.

B. Probable Cause Justifying Search of the Subject Device

7. In light of the foregoing, I believe there is probable cause that evidence of the Subject Offenses will be found on the **Subject Device**. As described above, in 2018 Schulte previously committed a number of offenses in connection with his efforts to disclose protected discovery materials and national defense information from the MCC: he possessed and used contraband cellphones in the MCC, he violated the Protective Order by sending a protected search warrant affidavit to a reporter, he engaged in a scheme to send protected discovery materials to WikiLeaks, and he disclosed and attempted to disclose sensitive national defense information about CIA personnel figures and cyber tools to the reporter and to social media users. More recently, Schulte appears to have manipulated the BIOS of the **Subject Device** in a manner that could allow him to overcome the "air gapping" of that computer and re-enable wireless services. Those wireless services could be used to access a WiFi signal that may reach the MDC or could be used with a contraband cellphone having "hotspot" capability to enable Schulte to access commercial mobile networks and mobile data networks, and provide him access to the internet. The fact that Schulte changed the user password on the BIOS and created

B-17

a large encrypted partition on the Subject Device hard drive indicates that he is seeking to conceal his activities, as well as any content that he may intend to communicate to third parties in violation of the SAMs, the Protective Order, and the laws against disclosure of classified information and national defense information. As also noted above, Schulte has used encrypted partitions in the past to protect and conceal contraband data, namely, child pornography.

8. Based on the foregoing, I respectfully submit that probable cause exists to believe that the **Subject Device** contains evidence, fruits, and instrumentalities of the Subject Offenses, including the following:

a. Evidence relating to the transmission of classified or unclassified discovery materials;

b. Evidence relating to the creation, use, deletion, or attempted creation, use, or deletion of encrypted partitions;

c. Evidence relating to alterations to the BIOS or operating system;

d. Evidence relating to use, access, or attempted use or access of wireless networks;

e. Evidence relating to the use, connection, or attempted use or connection of external devices to the **Subject Device**;

f. Evidence relating to the use or attempted use of the **Subject Device** as a means of communication with third parties;

g. Evidence relating to the identity or identities of the user(s) of the **Subject Device**;

h. Evidence relating to computers, cellphones, computer equipment, or online accounts and facilities (such as additional email addresses) controlled or maintained by the user(s) of the **Subject Device**;

i. Passwords or other information needed to access any such computers, cellphones,

B-18

computer equipment, accounts, or facilities, or to access any encrypted partitions or files on the **Subject Device**; and

j. Evidence relating to efforts to conceal any of the above evidence or conduct, including by deleting, destroying, hiding, removing, or encrypting evidence;

9. Accordingly, in light of the foregoing, I respectfully submit that there is probable cause to believe that Schulte has engaged in the **Subject Offenses**, as described in Exhibit A and paragraphs _ through _ above, that Schulte is the user of the **Subject Device**, and that the **Subject Device** contains evidence, fruits, and contraband relating to the **Subject Offenses**.

III. PROCEDURES FOR SEARCHING ESI

10. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the **Subject Device** for information responsive to the warrant.

11. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the **Subject Device** to locate all data responsive to the warrant.

12. In addition, the **Subject Device** will be reviewed by a Wall Team in order to identify and segregate material that reflects privileged attorney-client communications, attorney work-product, or trial preparation materials. Investigating agents may assist in efforts to decrypt encrypted data on the **Subject Device** so that the Wall Team can review the contents of any encrypted materials. The Wall Team will provide non-privileged materials from the **Subject**

B-19

Device to Schulte or, if he is represented by counsel in the underlying prosecution, to defense counsel in order to afford Schulte an opportunity to raise with the Court any objections to providing those materials to investigating agents and prosecutors on the prosecution team. Absent any such objections, the Wall Team will provide the non-privileged contents of the Subject Device to investigating agents and prosecutors on the prosecution team in order to review for evidence, fruits, and instrumentalities of the Subject Offenses two weeks after providing them to Schulte or to defense counsel of record.

IV. CONCLUSION AND ANCILLARY PROVISIONS

13. Based on the foregoing, I respectfully request the Court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

14. In light of the confidential nature of the full scope of the continuing investigation, including the continuing investigation of individuals to whom Schulte may have disclosed, intended to disclose, or attempted to disclose classified or protected materials, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that these papers may be provided to the FBI and any

B-20

personnel assisting in the review of seized materials, and may be produced by the Government to comply with any discovery or disclosure obligations in this matter.

/s/ Sean Collins

SEAN COLLINS
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to me
this 27 day of July 2022

Cheryl L. Pollak

THE HONORABLE ~~XXXXXXXXXX~~ Cheryl L. Pollak
UNITED STATES MAGISTRATE JUDGE

EXHIBIT ~~B~~ C

The unconstitutional 10/4/22 Search warrant

TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

APPLICATION FOR LEAVE TO FILE DOCUMENT UNDER SEAL

****
In the Matter of the Application of the United States of America for a Search Warrant for Premises Known and Described as Cell 801, Unit K84, located in Metropolitan Detention Center Brooklyn, 80 29th Street, Brooklyn, New York

22-MJ-1071
Docket Number

****

SUBMITTED BY: Plaintiff___ Defendant___ DOJ ✓
Name: Kaitlin McTague
Firm Name: USAO-EDNY
Address: 271-A Cadman Plaza East
Brooklyn, NY 11201
Phone Number: 718-254-6280
E-Mail Address: kaitlin.mctague@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES ___ NO ✓
If yes, state description of document to be entered on docket sheet:

A) If pursuant to a prior Court Order:
Docket Number of Case in Which Entered:
Judge/Magistrate Judge:
Date Entered:

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

Ongoing investigation

ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE, AND MAY NOT BE UNSEALED UNLESS ORDERED BY THE COURT.

DATED: Brooklyn , NEW YORK

10/4/22 Robert Levy
U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE
DATE

MANDATORY CERTIFICATION OF SERVICE:
A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, **B.)** ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation:_____; or **C.)** ✓ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

10/04/2022
DATE

Kaitlin McTague
SIGNATURE

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States of America for a Search Warrant for Premises Known and Described as Cell 801, Unit K84, located in Metropolitan Detention Center Brooklyn, 80 29th Street, Brooklyn, New York 11232, as well as Any Closed Containers/Items and Electronic Devices Contained in the Premises.

TO BE FILED UNDER SEAL

Agent Affidavit in Support of Application for Search and Seizure Warrant

Case No. 22-MJ-1071

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, VINCENT LAI, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been so employed since 2018. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. Since approximately January 2022, I have been assigned to the FBI's New York Field Office, Counterintelligence Division. During my tenure with the FBI, I have participated in counterespionage and counterintelligence investigations and, among other things, have conducted or participated in surveillance, the execution of search warrants, and the review of stored electronic information for evidence of crime. Through my experiences in the field and training relating to counterespionage and counterintelligence and related crimes, I am familiar with some of the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United

C-3

States by misusing their access to classified and national defense information. I am also familiar, though my training and experience, with the use of cellphones and computers in criminal activity and the forensic analysis of electronically stored information.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises described below (the "**Subject Premises**") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Premises

3. The **Subject Premises** is particularly described as Cell 801, Unit K84, located in Metropolitan Detention Center Brooklyn (the "MDC"), 80 29th Street, Brooklyn, New York 11232.

C. The Subject Offenses

4. I respectfully submit that probable cause exists to believe that the **Subject Premises** contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 401(3) (contempt of court), 1791(a) (possessing contraband in a correctional facility), 2252 (receipt, distribution, and possession of material involving the sexual exploitation of minors) and 2252A (receipt, distribution, and possession of child pornography), as well as

conspiracies and attempts to violate these provisions and aiding and abetting these offenses (the "**Subject Offenses**").

D. Terminology

5. The term "computer," as used herein, is defined as set forth in 18 U.S.C. § 1030(e)(1).

6. The terms "records," "documents," and "materials" include all information recorded in any form, visual or oral, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device), as well as the equipment needed to record such information (including but not limited to cameras and video recording and storage devices).

II. PROBABLE CAUSE

A. Probable Cause Regarding Commission of Subject Offenses

7. This application is in connection with the investigation of Joshua Adam Schulte for crimes arising out of his theft of classified, national defense information from the Central Intelligence Agency ("CIA") in 2016 and transmission of that stolen classified information to WikiLeaks.org ("WikiLeaks"); his obstruction of the investigation of those offenses in 2017; and his unlawful transmission and attempted transmission of additional

national defense information to a reporter and the public from prison in 2018 (collectively, the "Espionage Offenses"); and for crimes relating to his possession of child sexual abuse materials ("CSAM") both on personal computers owned by Schulte prior to his arrest in 2017 and on a laptop provided to Schulte for his use in Bureau of Prisons ("BOP") custody (the "Schulte Laptop") to facilitate his participation in the preparation of his defense of the Espionage Offenses (collectively, the "CSAM Offenses"). Since 2022, I have been involved in the investigation of those offenses as well as the jury trial of the Espionage Offenses beginning on June 13, 2022. *See United States v. Schulte*, S3 17 Cr. 548 (JMF) (S.D.N.Y.).[1] I have, among other things, reviewed prior applications for search warrants issued in connection with this investigation and records of court proceedings, and have spoken with other law enforcement officers as well as staff at the U.S. Attorney's Office for the Southern District of New York and the MDC. Based on my participation in that investigation, I have learned, among other things, the following:

a. In 2016, Schulte was employed by the CIA as a computer software developer. Schulte worked in the CIA's Center for Cyber Intelligence ("CCI"), which was responsible for the CIA's offensive cyber operations. Specifically, Schulte worked in the Engineering and Development Group ("EDG"), which produced computer programs, also known as "cyber tools," that other CIA components used in foreign intelligence cyber operations to collect intelligence from foreign adversaries and terrorist organizations. Schulte and other developers in EDG used a closed, classified CIA computer network, called DEVLAN, to develop and test these foreign intelligence cyber tools. On or about April 20, 2016, Schulte accessed a network location on DEVLAN where backups of certain development tools used by EDG were

[1] A trial of Schulte's CSAM Offenses and a copyright infringement offense is currently scheduled to begin on September 11, 2023.

stored and copied a set of backup files (the "Backup Files"). The Backup Files contained information about essentially all cyber tools developed or in development by EDG, including source code and documentation. Schulte later transmitted the Backup Files to WikiLeaks, which began releasing information from the Backup Files on its website on March 7, 2017. WikiLeaks continued to release data from the Backup Files on several occasions throughout 2017. WikiLeaks dubbed these releases "Vault 7" and "Vault 8." Schulte left the CIA in November 2016, after which he moved to New York, New York.

b. On or about March 15, 2017, the FBI executed a warrant to search Schulte's New York apartment. Among other things, a home computer (the "Home Desktop") was recovered as part of that search. The Home Desktop was later analyzed by FBI Computer Analysis Response Team ("CART") personnel and FBI computer scientists, who discovered multiple layers of encryption on parts of the Home Desktop internal hard drive.[2] One encrypted partition was found to contain over ten thousand images and videos of child sexual abuse materials (the "Home CSAM Files"). For example, one file was a video depicting a prepubescent female approximately three-to-six years old engaging in various sex acts.

c. On or about September 6, 2017, Schulte was charged in an indictment in the Southern District of New York with crimes relating to the receipt, possession, and transportation of child pornography. Following his arrest, Schulte was initially released pending trial subject to bail conditions. On or about December 14, 2017, Schulte's bail status

[2] The Home Desktop had multiple internal hard drives arranged in a RAID5 array, which is a protocol effectively allowing the computer to see all of the drives as a single drive, for various reliability and performance reasons. For convenience, the internal hard drive array will be referred to herein as the Home Desktop's internal hard drive.

was revoked and he was ordered detained pending trial. At that time, Schulte was designated to the Metropolitan Correctional Center in New York, New York (the "MCC").

d. In July 2021, Schulte was provided with the Schulte Laptop to review unclassified discovery pursuant to Rule 16 at the MCC. The Schulte Laptop replaced a prior discovery review laptop, was procured by his former counsel, the Federal Defenders of New York,[3] and was provided to the MCC by the U.S. Attorney's Office following a security inspection and "air-gapping," that is, the implementation of security settings and modifications intended to prevent the Schulte Laptop from being able to wirelessly connect to or access any computer network, including the internet.

e. In or about October 2021, following the closure of the MCC, Schulte was redesignated to the MDC. Since that time, Schulte has been housed in the **Subject Premises**. Schulte is the only inmate in the **Subject Premises** (*i.e.*, he does not have a cellmate). While incarcerated in the **Subject Premises**, Schulte's confinement is governed by Special Administrative Measures (the "SAMs") imposed pursuant to 28 C.F.R. § 501.2 and implemented by the BOP. In general, the SAMs prohibit Schulte from receiving material from other inmates, visitors, or any other individuals except as approved by the FBI and/or BOP, or from his attorneys, who may only provide Schulte with materials related to his defense, and who must affirm that they understand this restriction of the SAMs.

[3] In approximately July 2021, Schulte waived his right to counsel and proceeded *pro se*. Former counsel Sabrina Shroff and Deborah Colson were appointed as standby counsel. Following the jury's guilty verdicts at trial in July 2022 on all counts of the Espionage Offenses, *see infra* ¶ ___, Schulte requested that counsel be reappointed for all purposes except for post-trial motions pursuant to Federal Rules of Criminal Procedure 29 and 33. The District Court granted Schulte's request. Deborah Colson was relieved as counsel, and Schulte is currently represented by Sabrina Shroff and Cesar DeCastro.

f. Through the discovery materials loaded onto the Schulte Laptop, as well as additional external hard drives produced to him at the MCC and MDC, Schulte has had access to unclassified discovery materials in the **Subject Premises**. Based on my conversation with an official from the BOP, I understand that Schulte has maintained the Schulte Laptop in the **Subject Premises**, except when he has taken it to Court or when it has been necessary for him to provide it to BOP Staff to be recharged. I also understand that BOP Staff have observed Schulte frequently connect other hard drives and removable media to the Schulte Laptop while present in the **Subject Premises**.

g. Schulte has had access to classified discovery and to the contents of his home computer, which contains the Home CSAM Files, through regular visits to the courthouse Secured Compartmented Information Facility ("SCIF") at the Daniel Patrick Moynihan U.S. Courthouse, 500 Pearl Street, New York, New York; where classified discovery is available to him and defense counsel, and where a hard drive containing the Home CSAM Files is stored in a safe. Though the hard drive containing the Home CSAM Files contained no classified material, it was made available for Schulte's review in the SCIF in order to facilitate his trial preparation on the Espionage Offenses; and, in order to comply with Adam Walsh Act requirements, *see* 18 U.S.C. § 3509(m), was maintained in a dedicated safe whose combination was known only to the FBI and the court-appointed Classified Information Security Officer ("CISO"). The hard drive containing the Home CSAM Files could be viewed using a laptop made available by the CISO in the SCIF, which has since been used exclusively for that purpose and also maintained in the dedicated safe. Schulte's visits to the SCIF are monitored by video by members of the U.S. Marshals Service and the FBI.

C-9

h. On July 27, 2022, United States Magistrate Judge Cheryl L. Pollak of the Eastern District of New York signed a warrant authorizing the seizure and search of the Schulte Laptop, which was at that time located in the **Subject Premises** (the "Laptop Warrant"). The Laptop Warrant and the affidavit in support of the application for that warrant are attached as Exhibit A, and are incorporated by reference herein. As described in the Laptop Warrant, while Schulte was incarcerated at the MCC, he engaged in a variety of misconduct between 2017 and 2018, including:

i. Schulte procured a contraband cellphone that he equipped with a variety of applications designed to conceal his activity. (Exh. A ¶¶ 6(f)-(g)).

ii. Schulte attempted to procure a USB drive inside the MCC, and appears to have attempted to use the contraband cellphone to transmit protected discovery materials to WikiLeaks. (*Id.* ¶¶ 6(f), (l)).

iii. Schulte engaged in communications with a news reporter in which he disclosed information from search warrants that had been provided to Schulte in discovery that Schulte stated he knew was covered by a protective order entered by the Court prohibiting such disclosure. (*Id.* ¶ 6(h)).

iv. Schulte drafted a variety of handwritten materials intended for dissemination on the internet that included sensitive, classified, national defense information regarding the identities of CIA officers and the use of CIA cyber tools. (*Id.* ¶¶ 6(j)-(k)).

v. Schulte used an encrypted messaging application installed on contraband cellphones to transmit to a reporter both material marked "USG-CONFIDENTIAL" to indicate that it was covered by the protective order entered in this case and material containing sensitive national defense information regarding CIA networks. (*Id.* ¶ 6(m)).

C-10

i. On or about June 30, 2022, FBI Special Agent Evan Schlessinger testified at Schulte's trial. In his testimony, in relevant part and in sum and substance, Special Agent Schlessinger testified that he participated in a search of Schulte's cell at the MCC in or about October 2018. During that search, FBI agents recovered notebooks contained in Schulte's cell that included, among other things, handwritten passwords for accounts on encrypted messaging applications created by Schulte while incarcerated.

j. On or about March 9, 2020, Schulte was convicted following a jury trial of violations of 18 U.S.C. §§ 1001 (in connection with false statements Schulte made to the FBI during the investigation of the theft of the Backup Files) and 401(3) (in connection with Schulte's violation of the unclassified Protective Order entered in this case). On or about July 13, 2022, Schulte was convicted following a jury trial of violations of 18 U.S.C. §§ 793(b), 793(e), and 1030 (in connection with Schulte's theft and transmission of the Backup Files to WikiLeaks); 18 U.S.C. § 793(e) (in connection with Schulte's transmission of classified information to a Washington Post reporter while incarcerated at the MCC); 18 U.S.C. § 793(e) (in connection with Schulte's attempted dissemination of other classified information while incarcerated at the MCC); and 18 U.S.C. § 1503 (in connection with Schulte's obstruction of the grand jury investigation of the theft of the Backup Files).

k. As described more fully in the Laptop Warrant, during the pendency of Schulte's trial, the Government identified various ways in which Schulte appears to have manipulated the Schulte Laptop to evade controls designed to prevent its unauthorized use, including by modifying the Basic Input/Output System ("BIOS") and creating a large encrypted partition. (Exh. A ¶¶ 6(t)-(v)).

l. After the Schulte Laptop was seized pursuant to the Laptop Warrant, it was transported to the FBI office in New York, New York, to be searched.

m. On or about August 26, 2022, Schulte was produced to the courthouse SCIF and, during that visit, asked to view the hard drive containing files from the Home Desktop. Another FBI special agent provided the hard drive to Schulte and afterwards re-secured it in the dedicated safe. While securing the materials containing the Home CSAM Files, that other FBI agent observed that an unauthorized thumb drive (the "Thumb Drive") was connected to the laptop used by Schulte and his counsel to review the Home Desktop discovery hard drive containing the Home CSAM Files.

n. Pursuant to the terms of the Laptop Warrant, the initial search and review of the contents of the laptop for evidence of the subject offenses set forth therein, specifically violations of 18 U.S.C. §§ 401(3) (contempt of court) and 1791(a) (possessing contraband in a correctional facility), is being conducted by law enforcement agents who are not part of the prosecution team, supervised by an Assistant U.S. Attorney who is also not part of the prosecution team and is experienced in privilege matters (the "Wall Team"), to segregate out any potentially privileged documents or data. The Laptop Warrant further provides that, before providing any non-privileged materials to the prosecution team, the Wall Team will first provide them to Schulte and his counsel to afford them an opportunity to present the Court presiding over his case with any objections to the materials being turned over to the prosecution team.

o. I understand that, up to this point, the Wall Team has been able to review certain parts of the material extracted from the Schulte Laptop, but that the Wall Team has not been able to access the encrypted partition created by Schulte on the Schulte Laptop. Because of the nature of the encryption used by Schulte to create that partition, I understand that

C-12

it is unlikely that the Wall Team will be able to decrypt that partition without the password used by Schulte to encrypt it.

p. On or about September 22, 2022, a member of the Wall Team contacted me and another FBI special agent who is part of the prosecution team to advise that, during the Wall Team's review of the Schulte Laptop, they had discovered a substantial amount of what appears to be child sexual abuse materials (the "Laptop CSAM Files") and to request guidance about how to proceed. I and the other FBI special agent contacted the Assistant U.S. Attorneys assigned to this matter, who advised me that the Wall Team should stop their review to permit the Government to obtain an additional warrant authorizing a search for evidence of offenses involving child sexual abuse materials, and we conveyed that instruction to the Wall Team. Because the terms of the Laptop Warrant preclude the prosecution team from receiving the results of the Wall Team's search without first providing them to Schulte and his counsel, I understand that another Assistant U.S. Attorney was assigned to the Wall Team to be able to review the material and assist in obtaining that warrant.

q. Based on my conversations with a member of the Wall Team, I understand that an FBI agent experienced in offenses involving child sexual abuse materials has reviewed the Laptop CSAM Files and confirmed that, based on his training and experience, the Laptop CSAM Files include images that qualify as "child pornography," as that term is defined in 18 U.S.C. § 2256(8). In light of the terms of the Laptop Warrant, I have not yet personally reviewed the Laptop CSAM Files.

r. On or about September 23, 2022, United States District Judge Jesse M. Furman of the Southern District of New York signed a warrant authorizing the expansion of the search of the Schulte Laptop to include searching for evidence of violations of

18 U.S.C. §§ 2252 (receipt, distribution, and possession of material involving the sexual exploitation of minors) and 2252A (receipt, distribution, and possession of child pornography) (the "Laptop CSAM Warrant"). A copy of the Laptop CSAM Warrant and the affidavit in support of the application for that warrant are attached as Exhibit B and are incorporated by reference herein. Pursuant to the terms of the Laptop Warrant, the affiant on the Laptop CSAM Warrant was a member of the Wall Team, and I did not review the Laptop CSAM Warrant or the affidavit in support of that warrant before they were presented to the Court. I understand that, after the Laptop CSAM Warrant was signed by the Court, the Wall Team, in consultation with supervisors in the U.S. Attorney's Office, determined that the contents of the application in support of the Laptop CSAM Warrant did not contain any privileged information and could be provided to the members of the prosecution team, consistent with the modified privilege review procedures of the Laptop CSAM Warrant, which provide that material that the Wall Team determines (i) is non-privileged and (ii) appears to be potentially responsive to the subject offenses concerning child sexual abuse materials may be made available directly to the prosecution team without first consulting Schulte or his counsel. (*See* Exh. B, Attachment A ¶ III.3).

B. Probable Cause Justifying Search of the Subject Premises

8. In light of the foregoing, I believe there is probable cause that evidence of the Subject Offenses will be found in the **Subject Premises**. Schulte appears to have possessed contraband in the **Subject Premises**, in that he possessed the Laptop CSAM Files contained on the Schulte Laptop while housed in the **Subject Premises**. In addition, as described above and in the Laptop Warrant, in 2018 Schulte previously committed a number of offenses in connection with his efforts to disclose protected discovery materials and national defense information from

the MCC: he possessed and used contraband cellphones in the MCC, he violated the Protective Order by sending a protected search warrant affidavit to a reporter, he engaged in a scheme to send protected discovery materials to WikiLeaks, and he disclosed and attempted to disclose sensitive national defense information about CIA personnel figures and cyber tools to the reporter and to social media users. More recently, while housed in the **Subject Premises,** Schulte appears to have manipulated the BIOS of the Schulte Laptop in a manner that could allow him to overcome the "air gapping" of that computer and re-enable wireless services. Those wireless services could be used to access a WiFi signal that may reach the MDC or could be used with a contraband cellphone having "hotspot" capability to enable Schulte to access commercial mobile networks and mobile data networks, and provide him access to the internet, which is a potential source of the Laptop CSAM Files. In addition, the **Subject Premises** appear to contain other removable electronic media that Schulte has connected to the Schulte Laptop containing the Laptop CSAM Files, which may also be the source of the Laptop CSAM Files copied onto the Schulte Laptop or may contain copies of the Laptop CSAM Files transferred from the Schulte Laptop (in which case such media would itself be contraband), or other evidence regarding the transmission and/or possession of the Laptop CSAM Files by Schulte or others known and unknown. In addition, notes and other handwritten materials located in the **Subject Premises** may contain passwords or other information necessary to decrypt the encrypted partition created by Schulte on the Schulte Laptop, similar to how passwords for encrypted communications accounts created by Schulte were previously recovered from handwritten materials discovered during the 2018 search of Schulte's cell at the MCC.

9. Based on the foregoing, I respectfully submit that probable cause exists to believe that the **Subject Premises** contains evidence, fruits, and instrumentalities of the Subject Offenses, including the following:

a. Evidence relating to the transmission of classified or unclassified discovery materials;

b. Evidence relating to the creation, use, deletion, or attempted creation, use, or deletion of encrypted partitions;

c. Evidence relating to alterations to the BIOS or operating system of the Schulte Laptop;

d. Evidence relating to use, access, or attempted use or access of wireless networks;

e. Evidence relating to the use, connection, or attempted use or connection of external devices to the Schulte Laptop;

f. Evidence relating to the use or attempted use of the Schulte Laptop as a means of communication with third parties;

g. Evidence relating to other computers, cellphones, computer equipment, or online accounts and facilities (such as additional email addresses) controlled or maintained by Schulte or other user(s) of the Schulte Laptop;

h. Passwords or other information needed to access any such computers, cellphones, computer equipment, accounts, or facilities, or to access any encrypted partitions or files on the Schulte Laptop;

i. Originals, copies, and negatives of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

j. Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

k. Correspondence and records pertaining to violation of the Subject Offenses including email, chat logs, electronic messages, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

l. Communications with any minor from whom any child pornography, as defined by 18 U.S.C. § 2256(8), is solicited or received;

m. Any child pornography as defined by 18 U.S.C. § 2256(8);

n. Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);

o. Notes, documents, records, invoices, or correspondence, in any format and medium, including email, chat logs and electronic messages, and other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

p. Addresses, notes, names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and

q. Evidence relating to efforts to conceal any of the above evidence or conduct, including by deleting, destroying, hiding, removing, or encrypting evidence.

10. Based on my training and experience, I also know that, where computers are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.
- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in "slack space," until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created or viewed than on a particular user's operating system, storage capacity, and computer habits.
- In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

11. Accordingly, in light of the foregoing, I respectfully submit that there is probable cause to believe that Schulte has engaged in the **Subject Offenses**, as described in Exhibits A and B and paragraph 7 above, that Schulte is the sole occupant of the **Subject Premises**, and that the **Subject Premises** contains evidence, fruits, and contraband relating to the **Subject Offenses**.

III. PROCEDURES FOR SEARCHING ESI

12. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review." Consistent with

Rule 41, this application requests authorization to seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

a. First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.

b. Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

c. Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.

d. Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

13. Following seizure of any electronic media from the **Subject Premises** and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical

experts under government control) will review the ESI contained on any electronic media seized from the **Subject Premises** for information responsive to the warrant.

14. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

15. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from devices seized from the **Subject Premises** to locate all data responsive to the warrant.

IV. PRIVILEGE REVIEW PROCEDURES

16. Because documents, notes, electronic media, or other materials seized from the **Subject Premises** may contain material related to the preparation of Schulte's defense, the search of the **Subject Premises** and, subject to the provision in paragraph 17 below, the initial review of any seized materials, including electronic media, will be conducted by members

of the Wall Team in order to identify and segregate material that reflects privileged attorney-client communications, attorney work-product, or trial preparation materials. The Wall Team may confer with the investigating agents and prosecutors assigned to this matter to assist in identifying relevant materials potentially responsive to the warrant during the search, and investigating agents may assist in efforts to decrypt or otherwise access any encrypted data on seized electronic media so that the Wall Team can review the contents of any encrypted materials. The Wall Team will provide non-privileged materials from the **Subject Premises** to Schulte's counsel-of-record in *United States v. Schulte*, S3 17 Cr. 548 (JMF), in order to afford Schulte an opportunity to raise any objections to providing those materials to investigating agents and prosecutors on the prosecution team. The Wall Team will then turn over the non-privileged documents and data to the FBI case agents and prosecutors involved in the prosecution two weeks after providing those documents and data to Schulte's counsel, unless an objection has been made to the Court with respect to particular documents and data. The FBI case agents and prosecutors involved in the prosecution would review those documents and data for evidence of the Subject Offenses, as described above.

17. For any material that the Wall Team determines (i) is non-privileged and (ii) appears to be potentially responsive to the subject offenses relating to child sexual abuse materials (for example, the material appears to contain child sexual abuse materials), the Wall Team will make such material (and only such material) available directly to the prosecution team in this matter without first consulting Schulte's counsel.

V. CONCLUSION AND ANCILLARY PROVISIONS

18. Based on the foregoing, I respectfully request the Court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

C-21

19. In light of the confidential nature of the full scope of the continuing investigation, including the continuing investigation into whether and to whom Schulte may have disclosed, intended to disclose, or attempted to disclose classified or protected materials or child sexual abuse materials, or from whom Schulte may have obtained child sexual abuse materials, including but not limited to the Laptop CSAM Files, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that these papers may be provided to the FBI and any personnel assisting in the review of seized materials, and may be produced by the Government to comply with any discovery or disclosure obligations in this matter.

Vincent Lai

VINCENT LAI
Special Agent
Federal Bureau of Investigation

Sworn to me through the transmission of this
Affidavit by reliable electronic means, pursuant to
Federal Rule of Criminal Procedure 41(d)(3) and 4.1,
this 4th day of October 2022

Robert Levy

THE HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE

EXHIBIT D

10/5/22 Seizure Receipt

FD-597 (Rev 8-11-94) Page 1 of 1

P-1

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # 22-MJ-1071

On (date) 10/5/2022

item(s) listed below were:
- ☐ Received From
- ☐ Returned To
- ☐ Released To
- ☒ Seized

(Name)

(Street Address) Cell 801, Unit K84-MDC

(City) 80 29th St. Brooklyn, NY 11232

Description of Item(s): One WD Elements Drive
one notebook with handwriting
Four compact discs
Forty-six white sleeves with compact discs
Six compact discs
Twelve notebooks
Four DVDs
Documents, to include Secret//NOFORN and Confidential
Two DVDs

Received By: Manager (Signature)

Received From: No one present (Signature)